TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JUHA HEIKKILÄ

INFORMATION SECURITY RISK ANALYSIS AND MITIGATION METHODS FOR INDUSTRIAL INTERNET IN INDUSTRIAL VENDOR SEGMENT

Master of Science Thesis

Examiner: Professor Hannu Kärkkäinen
Examiner and the topic approved at the Council Meeting of the Faculty of Business and Technology Management on May 29th, 2017

ABSTRACT

JUHA HEIKKILÄ: Information security risk analysis and mitigations for industrial internet in industrial vendor segment.
Tampere University of Technology
Master of Thesis, 76 pages, 3 appendix pages
May 2017
Master's Degree Programme in Information and Knowledge Management
Major: Business Information Management
Examiner: Professor Hannu Kärkkäinen

Keywords: Industrial internet, information security, iot information security,

Finland is known for solid and big industrial vendor companies. Information technology changes industrial segment at the moment. Sensors are added to the industrial devices and all the information is communicated digitally to centralized storage. Devices can be monitored and controlled remotely using the collected data. At the same time cybercrime business is globally growing and smart industrial devices enables new way to attack companies. This research was done to understand what does Finnish industrial vendor companies think about cyber security threats and mitigation methods in industrial internet.

The research was conducted by using existing literature as a theoretical framework. Industrial internet system and its maturity is described in order to understand also information security around the industrial internet. After understanding industrial internet as a phenomena information security for industrial internet is described. Research gives a high-level understanding of cyber-security related risks and mitigation methods in industrial internet systems. Then the synthesis of theoretical framework was used in empirical part of this research. Six unstructured interviews were conducted for big Finnish industrial vendor companies. Interview included questions about company's industrial internet development, information security risks and mitigation methods.

According the interviews there are not so big information security risks that the industrial internet can be implemented as its fullest. Companies pointed that top business risks from cyber security attacks are related that their products could cause interruption for production or customer information could be leaked out. When companies are doing security work for industrial internet system digital identity, embedded security and physical threat are the top 3 information security risks. Industrial internet security work is focused a lot to sensor and transformation level in industrial internet architecture. In addition, active information security management process, security training for employees and reliable technology partners are in a key role for successful industrial internet information security work.

TIIVISTELMÄ

JUHA HEIKKILÄ: Teollisen internetin tietoturvan riskien tunnistaminen ja lieventäminen teollisten laitetoimittajien segmentissä
Tampereen teknillinen yliopisto
Diplomityö, 76 sivua, 3 liitesivua
Toukokuu 2017
Tietojohtamisen diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tiedonhallinta
Tarkastaja: professori Hannu Kärkkäinen

Avainsanat: teollinen internet, tietoturva, iot tietoturva

Suomi tunnetaan isoista ja vakaista teollisuuden laitetoimittaja yrityksistä. Tällä hetkellä tietotekniikka muuttaa teollisuuden segmenttiä. Sensoreita lisätään teollisiin tuotteisiin ja kaikki niiden keräämä informaatio tallennetaan keskitettyihin pilvipalveluihin. Teollisia laitteita voidaan etänä ohjata ja seurata teknologian ansiosta. Samaan aikaan kyberuhkien ja hyökkäysten määrä kasvaa maailmalla ja lisääntyvä määrä älykkäitä teollisia laitteita avaa yrityksistä hyökkäyspinta-alaa kyberhyökkäyksille. Tämä tutkimus tehtiin, jotta voidaan ymmärtää mikä on suomalaisten teollisten laitetoimittajien käsitys teollisen internetin tietoturvasta ja sen suojausmenetelmistä.

Olemassa olevia tutkimuksia ja kirjallisuutta käytettiin teoreettisen kehyksen luomiseen. Koska tietoturvallisuutta käsitellään tutkimuksessa suhteessa teolliseen internetiin, teollinen internet ja sen maturiteetti on avattu teoreettisessa viitekehyksessä hyvin. Kun teollinen internet ilmiönä tunnetaan, kerrotaan teollisen internetin tietoturvasta. Tutkimus antaa korkean tason ymmärryksen teollisen internetin tietoturvauhkista ja niiden mitigointi-menetelmistä. Teoreettisen viitekehyksen jälkeen teetettiin puolistrukturoituja haastatteluita kuudelle suomalaiselle teolliselle laitetoimittajalle. Haastattelut sisälsivät kysymyksiä teollisen internetin kehityksestä ja maturiteetista. Tämän lisäksi tarkasti käsiteltiin teollisen internetin tietoturvaa liiketoimintariskien ja konkreettisten tietoturvariskien näkökulmasta.

Haastattelujen mukaan ei ole olemassa niin suuria tietoturvauhkia, että teollisen internetin potentiaalia ei pystyisi ottamaan käyttöön niin kehittyneesti kuin mahdollista. Yrityksen osoittivat, että suurimmat liiketoimintariskit teollisen internetin tietoturvassa on tuotannon jatkuvuuden ongelmat ja asiakasdatan vuotaminen. Kun yritykset tekevät teollisen internetin tietoturvatyötä identiteetinhallinta, sulautettu ja fyysinen turvallisuus ovat kolme suurinta mainittua tietoturvauhkaa. Teollisen internetin tietoturvatyö keskittyy laitteisiin ja niiden liikenteeseen pilveen asti. Tämän lisäksi tutkimuksessa tuli ilmi, että aktiivinen tietoturvan hallinnan prosessi, työntekijöiden kouluttaminen ja luotettavat teknologia kumppanuudet ovat avainasemassa tietoturvatyö onnistumiselle.

PREFACE

Writing this research was a really good way to prove my endless interest for the world of IoT and cyber-security. Along this research, I met really inspiring people when I was doing the company interviews. I also got the feeling that this topic was important for interviewed people also. As having a relative solid work experience already in sales and marketing, this research allowed me going more closely to the subjects I have been studying in University as a technical point of view. This has been really fruitful. This research was a project for me that had been left hanging after active university studies when the work life took my time strongly few years back. This research proves me that I am able to stretch myself during my free time despite a full-time job. I certainly after this research can use the same extra energy used for this to develop myself towards my goals.

First I want to thank my examiner Hannu Kärkkäinen which was really helpful during the project and it was really efficient to work with him. Hannu had time for me even at short notice times. Special thanks to all the interviewed people who were able to give their precious time for this research. I hope the results will also help them with their own work.

Now when this research is finishes, I am ready for new challenges.

Helsinki, 21.5.2017

Juha Heikkilä

SISÄLLYSLUETTELO

APPENDIX A: SEMI-STRUCTURED INTERVIEW

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

ADC	Analog-to-Digital converter changes analogical signal such as temperature to digital signal which can be digitally transferred and stored.
API	*Application Programming Interface* means software interface which enables the integrations between applications and cloud services.
DoS	*Denial of Service* is a cyber security attack where attackers are trying to make applications or services unavailable. This is usually done by flooding.
GDPR	The *General Data Protection Regulation* is a regulation by European Parliament for strengthen and unify data protection for all individual in European Union area.
ICT	*Information and Communications Technology* means technology and machines that enables digital communications and processes.
IoT	*Internet of Things* means any digital or not digital object, e.g. household appliance, to connect Internet and communicating with each other in order to participate business processes.
IIoT	*Industrial Internet of Things* is Internet of Things in industrial segment. Industrial machines and sites are connecting the internet, creating their own connected systems. Can be also said as Industrial Internet.
M2M	*Machine-to-machine* means automatic communications between machine without human interface.
UI	*User Interface* is a way how humans and machines interact in order to operate and control.

1. INTRODUCTION

1.1 Motivation and background

World is changing faster than ever and the new industrial revolution is coming. Technological development enables today that everything can be connected into the internet. At the moment people can socialize, work and shop through internet, but what will happen when machines are talking with each other's? (Saarelainen & Collin, 2016; Kumar & Patel, 2014)

In industrial sector, companies see the potential of re-shaping the markets, make value and growth and competitive advantage with 'connecting the unconnected'. In Finland, industrial internet revolution has identified as one of the key themes by the Prime Minister's office. It is said, that Finland will be the future Silicon Valley of industrial internet.

However, this trend brings also a big elephant on the table; cyber security. When millions of devices are connected to the internet, it reveals a lot of attack surface for attackers. One of the finish industrial internet visionary and business man Pekka Lundmark has said that industrial internet will rise or fall over the data security (Lehto, 2015). Also, World Energy Counsel warns that the sector is prime target for cyberattack (World Energy Council, 2016). For example, in June 2010 Iran was attacked by the worm called Stuxnet and it destroyed Tehran's 1000 nuclear centrifuges and set back Iran atomic program over two years and the worm also infected over 60,000 computers beyond the plant (Telegraph, 2010). In 2015, Ukrainian electric power sector was attacked with custom malware and 80,000 people were without electricity over six hours (Zetter, 2016). Knowing the attack risks, companies need to be prepared. This research will go behind the curtains of manufacturing companies in Finland and helps to understand what are the cyber risks for industrial internet and how the risks are understood. (Saarelainen & Collin, 2016; Lehto, 2015)

The main motivation behind the cybercrime is money. The Jupiter Network research estimates that the cybercrime will cost companies total \$2.1 trillion by the year 2019 (Rooheart, 2017). Being a cybercriminal also known as a black hat hacker does not need very special skills. Hacking tutorials and black markets for cybercrime are reachable with internet connection. In many cases the risk is really low and risk of getting caught is significantly lower than with traditional criminal. Countries with most hackers are mostly poor ones for example Russia, China, Nigeria, Vietnam and Romania (Rayman, 2014). Poor countries are unable to afford specialized technologies to deal with hackers. According to PWC study (PWC, 2016) in 2016 46% of internal actor and 41% of external actor, this means that almost half of the fraudsters came from the same organization. The number of external fraudster are increasing, mainly because global network availability and computing skills.

Industrial sector is changing currently from embedded systems to IP-based cyber physical systems. According PWC's study (PWC, 2016) some industry sectors have experienced increase of crime incidents in the past 24 months. These industry sectors are aerospace & defence, manufacturing, transportation & logistics and energy industry. Hackers have found out that many suppliers have gaps in their security which can be easily exploited. This was not an issue before, because devices were connected in a closed system or did not have intelligence at all. Cisco predicts (Evans, 2011) that there will be roughly 50 billion devices connected to the internet by the year 2020 and Hewlett Packard study (Miessler, 2014) reveals that 70% of Internet of Things devices are vulnerable to attack. And this is not only a consumer problem, companies need to look carefully also their industrial systems with the same risk. So, when cybercrime business is booming and hackers will have more and more unprotected devices to play with, how are the companies prepared for the attacks?

In this research, I will dive into Finnish industrial vendor industry. At the moment, industrial internet hype is tangible and companies are in different states of creating new business value with connecting devices. How have companies prepared for the change and the risks and how the companies see different risks? This research will help to understand what is the industrial internet, what is a theoretical framework for securing the industrial internet and how have Finnish industrial vendor companies understand and are prepared for cybercrime.

1.2 Research goals and structure

The goal of this study is to create a mutual understanding between industrial internet and main cyber risks.

The main goal can be derived for one research goal (RG):

> **RG1**: *What are industrial internet information security risks and how they should be mitigated in Finnish industrial vendor segment?*

Research goal is an outcome from different research questions. Research will give answers to these research questions (RQ):

> **RQ2**: *What kind of information security risks appears in different levels of industrial internet architecture?*
> **RQ3**: *Why is it important to invest in industrial internet cyber in industrial vendor segment?*

> **RQ4**: *What is the role of industrial vendor company in industrial internet information security?*

In order to answer the main research questions, research must be broken into different sections. Firstly, research sets up a theoretical framework for the research. Theoretical framework answers to these sub-questions (SQ):

> **SQ1**: *What is industrial internet by architecture and maturity?*
> **SQ2**: *What kind of cyber risks there are in industrial internet?*

These sub-questions are extensively answered in theoretical framework (Sections 2 and 3). Framework creates a steady platform to implement the information towards the research questions and goals.

Work order of this research is firstly answer to theoretical framework, then for the research questions and lastly pull together answer for the research goal.

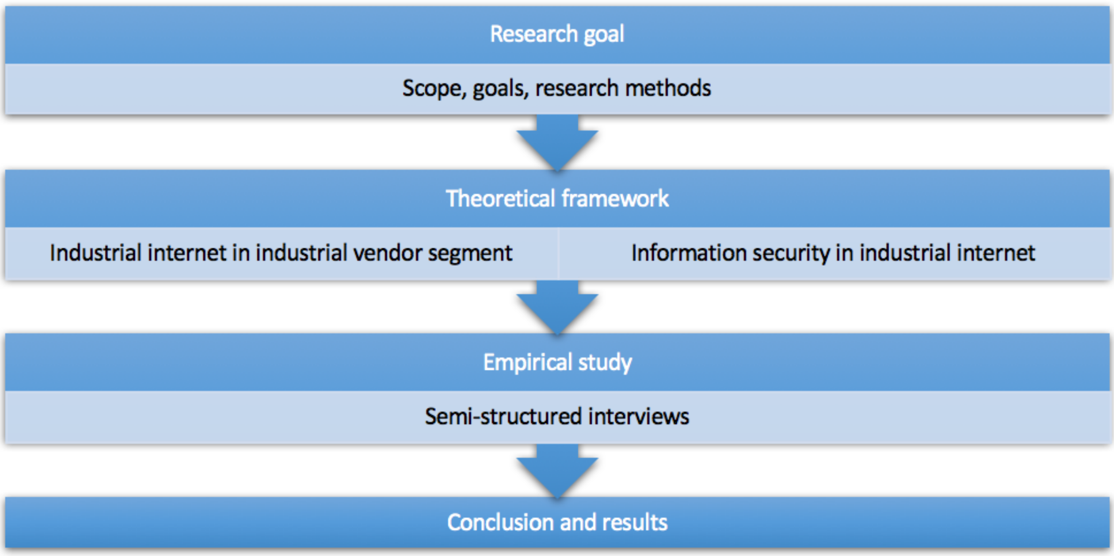


Figure 1. *Work order*

1.3 Scope and limitations

The world of Internet of Things is wide. Internet of Things will affect both consumer and business segments and there are plenty of applications.

This research is focused with the manufacturing category. Even inside manufacturing segment there are many applications like factory floors, industrial automation vendors and industrial vendors. Scope of this research is industrial vendors. In Finland, industrial vendor companies have already woken up for the industrial internet change.

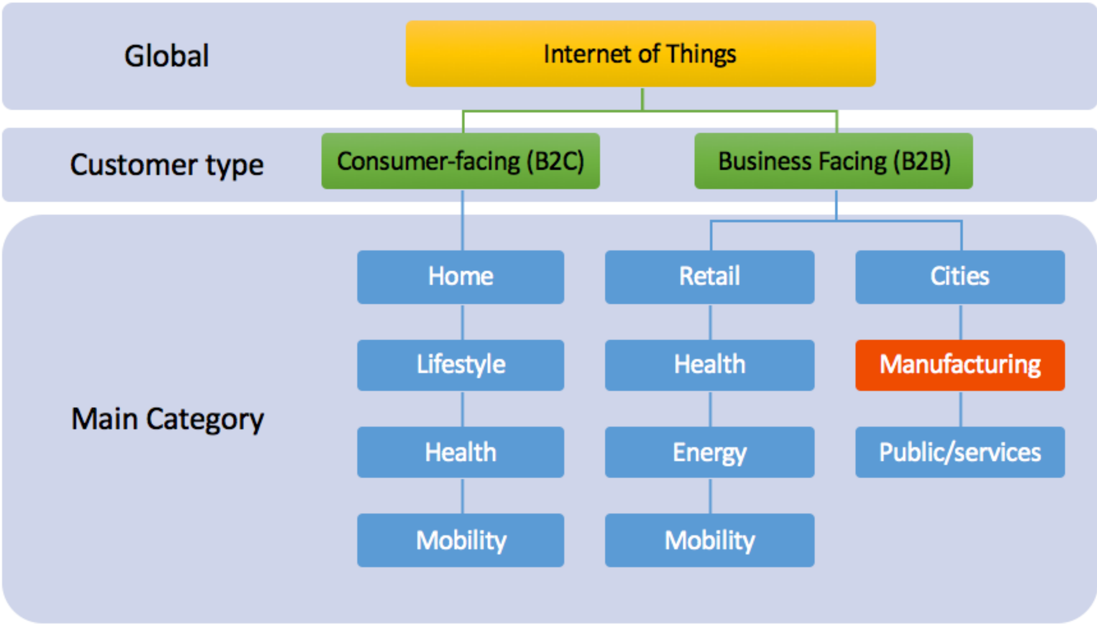


Figure 2. *IoT market segmentation (Lueth, 2014)*

Finland is an interesting market to explore industrial internet related topics. There is global manufacturing companies and huge amounts of technology and software expertise. According to Accenture and Frontier Economics research about industrial internet growth opportunities Finland ranks third after United States and Switzerland (Miessler, 2014). In Finland, there is ongoing my different kind of growth programs. In 2008 FIMECC (Finish Metals and Engineering Competence Cluster) was found to make Finland a recognized leader of industrial internet business.

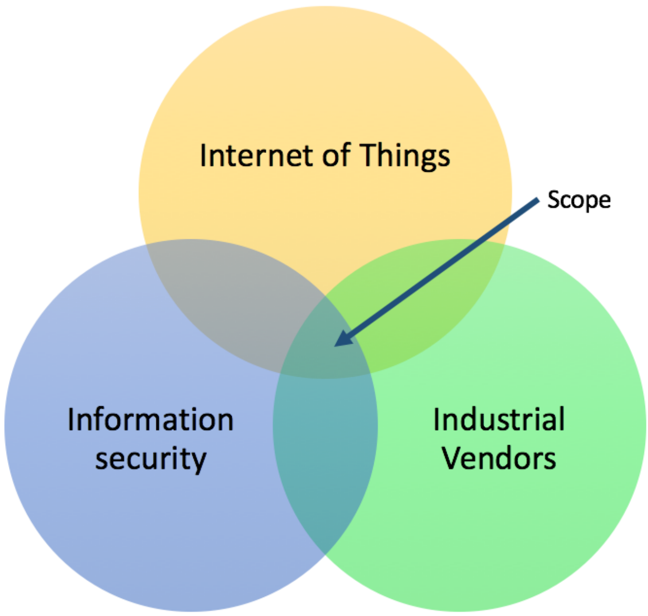


Figure 3. *Scope of the research*

Many of the global finish manufacturing companies have a strategy for the industrial internet. They have completed many different kind of industry hacks to innovate their business models and development. This research is focused on industrial vendor companies. It means that they have specific industrial internet architecture. They produce industrial goods for bigger entities, e.g. cranes for harbours. That means that products will have smart connections within the factory, customers, supply chain, maintenance and producers. Of course, most of the companies have their own production plants but this research will focus on the ecosystems created by the end products.

1.4 Research methodology

In order to make right conclusions in the research we need to compare different kind of philosophes and approaches.

This research is based on qualitative data collection. Objective is to gain an understanding of underlying reasons, beliefs and motivation behind industrial internet cyber security. (Hennink et al., 2010). The main research goal is to find out why to invest to information security in industrial internet. The problem is that there is no unified method to ensure the security of industrial internet. That's why it is really important to understand the beliefs and feeling inside interviewed companies.

Research consist theoretical framework and empirical section. Theoretical framework creates a ground to examine research questions. In empirical sections Finish industrial internet companies in the segment of industrial vendors.

Empirical information was collected with semi-structured interviews. Interviews were completed with a list of questions and specific questions, but there might be some variates between the interviews, depending on what topic there is some extra information. That way interviews can be also lead by respondents' priorities and opinions of the subject. With semi-structured interviews, we can examine the topic deeper and maybe find out something that was not able ask within the question frame. This is because interviewed companies are not in the same level of industrial internet an understanding how do the Finnish industrial vendor companies are understanding the cyber risks of industrial internet.

Table 1. *Summary of research methodologies used*

Concept	**Methodology**	**Effect to research**
Philosophy	• Hermeneutics	Qualitative research method which enables to gain deep understanding

		around the subject using subjective interpretations.
Approach	• Qualitative • Deductive	Enables to increase overall understanding of the topic. Can explore expressions and culture behind the questions from the organizations and motivations. Deductive approach refers to logical thinking and analysis of the results.
Information gathering and analysis	• Existing research literature and articles for theoretical framework • Semi-structured interviews for gathering empirical information • Empirical information and theoretical framework are combined and analysed together.	In the research two different kind of theoretical basis are combined. In order to answer research goal, information must be gathered from different organisations. Strategy is to use semi-structured interviews which is not a survey and goes not under case study strategy.
Results and conclusions	• Results is understanding the role of information security in industrial internet projects • Conclusions about how information security is felt with industrial internet business	Results of the research are overall making a better understanding of the subject Interviewed companies are summarized organizationally about the results and how did the companies answers compared to other companies.

2. INDUSTRIAL VENDOR IIOT

2.1 Definition of Industrial Internet

First time industrial internet was introduced in 2000 with Frost & Sullivan article, back then industrial internet applications were really expensive and difficult to implement, even if the applications were pretty simple. After 12 years Evans (Evans & Annunziata, 2012) introduced term industrial internet second time with his famous GE article and then the timing was right. According Evans, industrial internet has three key elements; intelligent machines, advanced analytics and people at work. In the past decades, there are lot of technological innovations around computing, network connections and the Internet. Now those innovations can be combined into most industries. Intelligent machines mean connecting the world's machines, platforms and facilities with sensors and software. The low-cost and level of connectivity around sensors and IT-systems is propitious. Advanced analytics means the advanced ways to perform physic-based analytics, predictive algorithms and deep engineering know-how about material science, electrical engineering and production. People at work refers to connecting people and allowing better service quality and security. (Evans & Annunziata, 2012)

Industrial Internet Consortium, IIC, has defined industrial internet like this (Industrial Internet Consortium, 2015):

"The Industrial Internet is an internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes. It embodies the convergence of the global industrial ecosystem, advanced computing and manufacturing, pervasive sensing and ubiquitous network connectivity."

Today there are many interconnected systems, which uses software, sensors and databases. But these industrial control systems have not been connected to wider systems or with the people working with them. (Industrial Internet Consortium, 2015) Industrial Internet brings Industrial control systems online to form large systems and connecting with people and analytics solutions. According Industrial Internet Consortium Industrial Internet systems cover energy, healthcare, manufacturing, transportation and related industrial systems.

Term machine-to-machine also known as M2M means communication between machines and also according to Saarelainen (2016) the term is in many ways synonym with industrial internet from a narrow point of view. Machine-to-machine refers to advanced and autonomous machine communications between each other's via connected software and artificial intelligence.

It is good also to define the difference between Industrial Internet of Things and Internet of Things. IIoT is defined as a part of Internet of Things. Internet of Things means connecting any unique device with the communications protocol. Common factor is also that things communicate with each other and with the systems and cloud services, where the data can be saved and analysed. Internet of Things is an umbrella term and industrial internet is one theme under it. According the ETLA report (Juhanko et al., 2015) industrial internet means likewise the business perspective of the whole Internet of Things and rest means consumer perspective. Also, the government gives their own additions with the terms information society when open data is connected with public sector services. With the industrial internet, the expected life cycle is assumed to be decades and with the consumer business life cycle is a lot faster (Saarelainen & Collin, 2016).

Industrial internet still does not achieve its goals when companies have connected devices with data management and applications. Industrial internet is actually born when business processes, products and services are connected to the network and the ensemble is creating databased services. The difference between todays industrial internet and old-style industrial control systems are that in ICS systems software was embedded into the products and with industrial internet products and services are embedded with software. So, software defines what are the features at that time. (Saarelainen & Collin, 2016)

According Porter and Heppelmann (2014) industrial internet is all about how smart, connected devices change interfaces of industry sector and reshapes industry sector. Briefly new relationships, new processes and new structures for business are created with three core elements; physical components, smart components and connectivity components. Porter and Heppelmann ground their definition more business perspective. They see that the technology offers a radical shift for industry and business processes, value and supply chains must be rethought. This also questions the organizational structures and strategies.

2.2 Fourth industrial revolution

Megatrends are born when structures of global society are examined from economic, social, technological or political point of view. Different industries, people and society structures are affected with megatrends are the trends are usually proceeded long before noticing.

The world is facing a new era of innovation in industry sectors. Before exploring the industrial revolution, it is good to define the facing changes of the world. Three key megatrends are globalisation, digitalisation and urbanization (Juhanko et al., 2015). The consequence of these megatrends is that people are acting differently and new kind of value and supply chains are innovated. Also, megatrends with environmental aspects like global warming are indirectly affecting with industrial revolution development. At the moment digitalisation enables industry sector to take the next step.

The main drivers enabling the revolution:

- Sensors fall in the price, low-power and better performance
- Internet enabling explosive growth of connected devices
- Big data, analytics and storage price decrease
- Consumer awareness and user interfaces
- Business acceleration (Saarelainen & Collin, 2016).

First industrial innovations were happened in the end of 1700 century when steam machines were invented and adapted into factory facilities. The main theme back then was that the machines were creating power for the first time with the mechanical automation. The second industrial revolution was completed with electrical power and that enables mass production and more advanced production lines. Third revolution was born when electronics and IT were implemented with the automation.

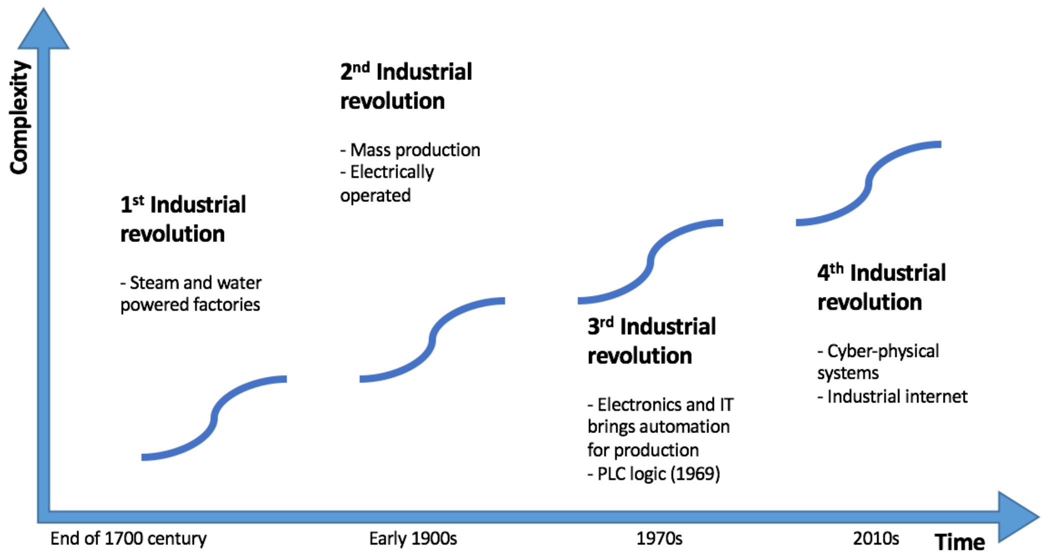


Figure 4. *Four industrial revolutions (Saarelainen & Collin, 2016)*

Fourth industrial revolution is also known as industry 4.0 is an on-going smart change through cyber-physical systems (Lee, 2014). Like said before, revolution is possible today because of the software development. The term Industrie 4.0 is the most known strategic initiative to exploit the potential of the industrial internet. Originally Industrie 4.0 is invented in Germany in 2013 as their principal project (Juhanko et al., 2015). This national development program is defined same way as the industrial internet. The goal is to emphasize the enhancement and optimization of industrial manufacturing systems with these basic elements; sensors, operating devices, local intelligence, communication networks, cloud technology, analytics and analytics-based decision-making. (Juhanko et al., 2015). According Technische Universität Dortmund (Hermann et al., 2015) Industrie 4.0 includes six main design principles:

Table 2. *Industry 4.0 six design principles*

Interoperability	Ability to connect and communicate between cyber-physical systems, smart factories and people. Standards will be key success factors with connecting these things.
Virtualization	Virtual copy and simulation models of smart factory which is created by connecting physical world sensor data with virtual models and simulations. Humans are supporting with this principal.
Decentralization	Autonomous decision-making by the embedded devices and systems. For quality and traceability, it is important to keep track the whole systems all time.
Real-time capability	Capability to collect and analyse data and offer derived results in real-time. And the factory is permanently tracked and analysed.
Service orientation	Offering services over IoT and can be utilized by the other participants and offer customer specific requirements.
Modularity	Flexible adoption of smart factories with replacing or expanding unique modules. With good modularity, seasonal fluctuations and changed products are easily managed.

Software development is the main key while examining the 4th industrial revolution. Software enables most of the industrial internet features. Even if the revolution is possible by the technology, it is important to keep business value creation, business models and service-culture in the core (Saarelainen & Collin, 2016).

2.3 Industrial internet maturity and future

Near past in industrial sector there was two business participants; the producer and the user. Added value is based from the physical use of the technology. Today industrial vendor companies are developing services and integrating their technology into system level solutions. Competition drives towards system level industrial internet solutions in order to bring customer value. Service provider gets huge amount of information about the use and operations of the services. Every customer gets information from used products, maintenance status alerts and abuse of the devices. Also, customer can make changes with the configurations of the used services. Industrial internet development can presented with steps. This development is described in this section as a maturity model of industrial internet. (Juhanko et al., 2015; Viitamo, 2014) Industrial internet maturity model is important to this thesis, because information security risks and mitigations are reflected to the maturity model.

Companies are not able take the full capability of industrial internet in use immediately. Product and business development happens in cycles and the business models also grows with the rest process. The maturity of the industrial internet can be described with following evolution:

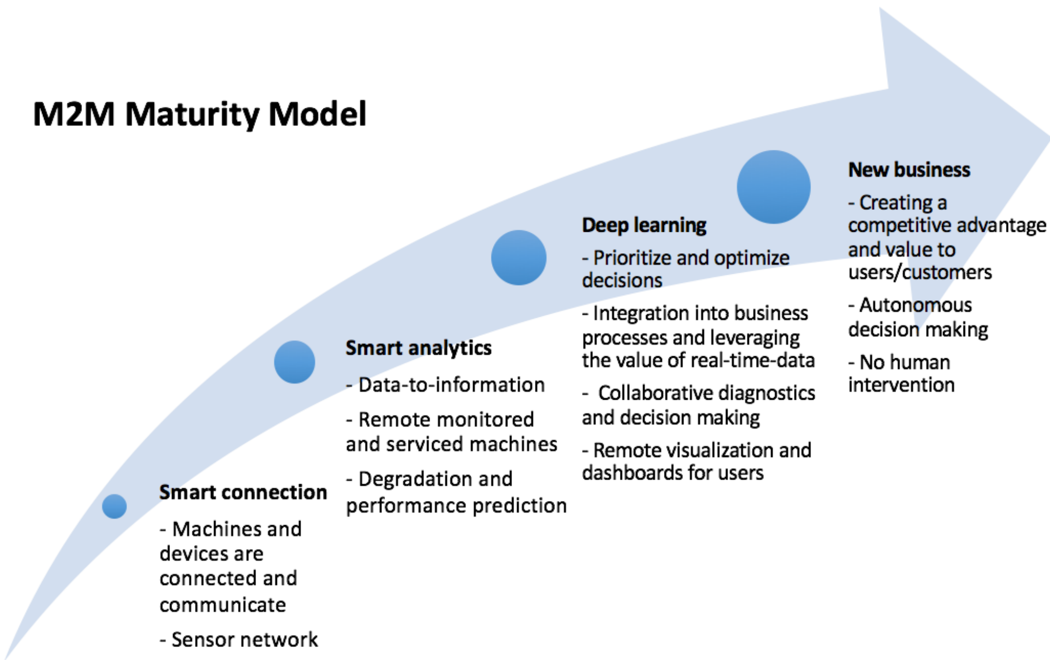


Figure 5. *M2M Maturity model. (Shan, 2015)*

In general, maturity is related to technological capabilities. Firstly, machines and devices are connected and then sensor-created data and background system data are stored, devices remotely monitored and creating information of the data. After this foundation, deeper business value-adding opportunities can be created. Data analytics, algorithms and software applications industrial internet can be implemented with higher maturity. Then business processes, decision making processes can be outsourced for the systems. At the highest level, autonomous decision making is implemented and human intervention can be totally taken out of. This is important to understand in this context, because also the information security risk and methods, which are described later on, can be different in every level of maturity model.

Always getting to the next step require prior step elements to be implemented and taken over new capabilities. These steps are so called change drivers which means that realization of capabilities of certain step company can have a transition to the next level. It is not default that companies are aiming for the highest point of the maturity model. Positioning should be a strategic choice within this scale, but practically developing with maturity means that companies have to adjust their business processes with the whole value chain and with the organisations dealing with the process. Of course, changing business models often means new competition. Also, market and innovation potential grows when company grows the maturity from embedded systems to open environment (Juhanko et al., 2015).

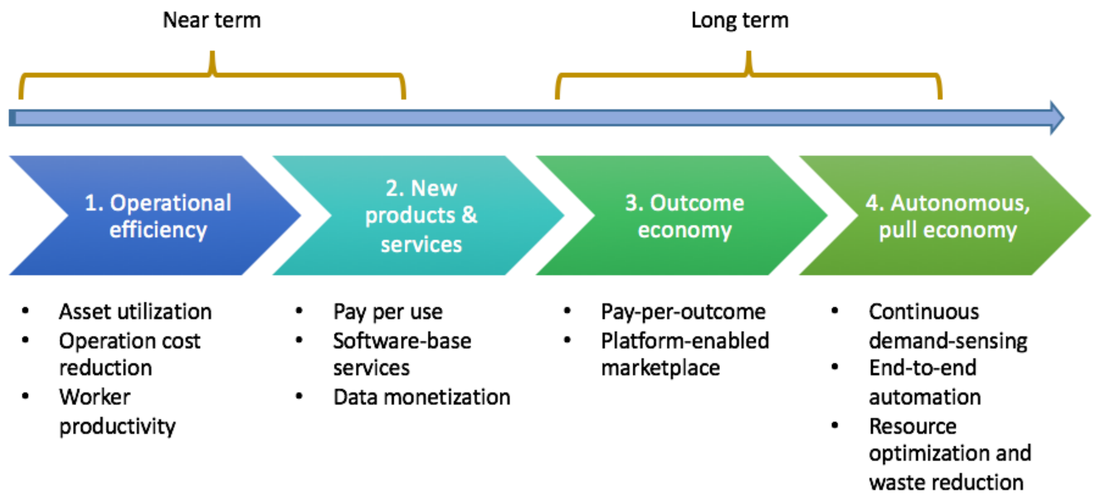


Figure 6. *The adoption and impact path (World Economics Forum, 2015)*

Figure 6 shows basically how the future will likely follow. Perspective is a bit same with the maturity model (Figure 5) but it gives options also with new business models. As figures shows business models are highly dependent of the technology maturity. For many companies' operational efficiency and smart connections are not new opportunities, most of the big players have had these technologies already about 20 years. But the new factory in this sector is the data management, big data and cloud based services. To create future business models, highly sophisticated algorithms and analytics are implemented.

Examining Figure 6 the near-term goals can be achieved within 2 years of industrial internet development. According World Economics Forums research (World Economics Forum, 2015) the long-term disruptions will occur in five years. Long term goals are more challenging steps towards new business models, because data management and analytics are far more complex than low-maturity development. The goal is to create value-adding models with data. Value adding model is not selling just the equipment but the pricing is based for example the use or production value.

When creating and implementing new business models it is vital to understand the effectiveness for the supply and subcontracting chains. The paradigm of these chains should be from a hierarchical network to service network. The formation of service networks contributes the industrial internet business model development.

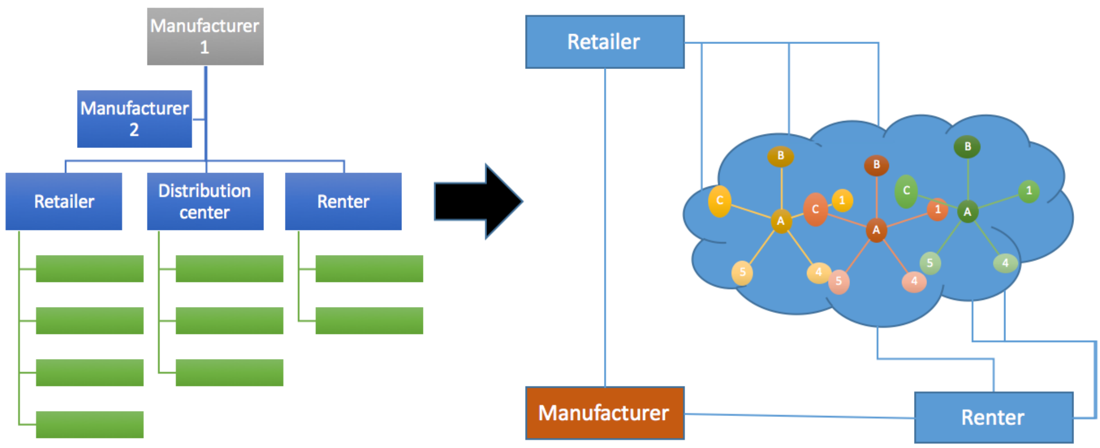


Figure 7. *From supply chain to service network (Mountreuil, 2012)*

Figure 7 visualizes the change from original supply chains to service networks. Service network is created when smartly linked users are exploiting open interfaces of service network. Instead of ordinary buying and selling process, implementing product functionality is highlighted for example via renting collaboration use.

For industrial internet, there are many areas of applications, but there are some more adapted models which are presented below; asset management, predictive maintenance, smart factory and service business. But of course, outside of these four models every company is thinking how to create most value-adding model for their own benefits.

Asset management

Asset management means that company has clear and exact view of their own assets and their manufactured products. Asset management requires that devices are equipped with sensors, connected to internet and cloud based services. As a result, company can get the following features possible (Saarelainen & Collin, 2016):

- Remote optimization
- Remote management
- Remote updates
- Remote control and remote use control

In this phase, industrial internet maturity is very low but companies can gain big value of getting connected remotely with their assets.

Remote controlling means the information about who, when and where the device is used. Then company can ensure that users have authority to use the product. Improper use can be stored to the system and can be used for example user training purposes.

The other perspective of the asset management is gaining performance information of the products. With the information abuse, can be analysed and overall performance can be analysed from the whole life cycle. This helps to development of the products and finding and refining troubleshooting.

Remote management means that user is able to control device or processes remotely. Management is using the product, and optimization is about the device configuration. Productivity and revenue are increased during the process. Remote updates enable to remotely update devices even to sensor level. This is important, because devices contain a lot of software.

Predictive maintenance

Predictive maintenance is one of the biggest industrial internet opportunities. Companies are expecting to gain utilization, prevent interruptions in production and to speed up maintenance shutdowns. Usually predictive maintenance is the first application area for companies when entering the industrial internet era. Predictive maintenance means that machine or device maintenance-need is solved from the real-time information. Sensor data with history gives the status of the condition of the machine, and it is reasoned when should it maintain. Predictive maintenance includes parts of the asset management. In predictive maintenance alarms are set when pre-defined limit-values are violated. In predictive maintenance analytics are used to find anomalies from the data automat. Goal is to maximize device capacity and ensure its stability. Manufacturing companies and vendors can have quick wins in this area, but it means that the analytics and knowledge of the devices are strong. Usually collecting the history data slows down implementing predictive maintenance as its full capacity, because in order to analyse data there must be a lot of history data. (Saarelainen & Collin, 2016; Juhanko et al., 2015)

Industrial internet era predictive maintenance replaces old ways of doing the maintenance. Traditional and old preventive maintenance actually means that there is service offer before the faults. In time-based maintenance service is offered by pre-scheduled timing or e.g. certain machine-time is exceeded. But industrial internet offers now that condition-based maintenance can bring into play. The benefits of the predictive maintenance are (Saarelainen & Collin, 2016):

- More efficient use of machines
- Reduce maintenance expenses
- Reduce unpredictable disorders
- Prevent degradation of the equipment
- Identify underperforming devices
- Improve the quality of production

- Machine anti-aging
- Need-based maintenance
- Reduce maintenance travel expenses
- Release spare parts capital

The benefits of predictive maintenance show that it really offers significant monetary benefits.

Service business

When manufacturer have the outlook to their devices the business earning models can also be customized by the need. For example, manufacturers can sell their products as “product-as-a-service” which means that invoicing of the devices is based on operating hours, volume of the production or even on reduction in production downtime. There is then lower threshold to buy the products (Saarelainen & Collin, 2016). This type of invoicing is called also by “pay-per-outcome” or “pay-per-use” (Mountreuil, 2012).

When manufacturers can analyse the data, and run predictive maintenance, they can also offer “after-sales” products. For example, they can offer analytics based remote optimization and updates. And of course, new applications can be created, which can help customers e.g. manage their products with mobile interface. Also, the sensor-data as a big mass enables trading. This offers also 3rd party players to create applications with the data. (Saarelainen & Collin, 2016)

Fleet management means that device supplier collects database from supplied devices, owners, locations and maintenance. With that information spare part sales, maintenance and other services can be developed. Fleet management can be also used as operational purposes like device management. (Juhanko et al., 2015)

Smart Factory

Smart factory means a factory where every single device is sensored and connected into same network, database and analytics platform. The wholeness makes factory adaptable and releases human interface from adjust and monitoring. Smart factory adapts according the production and it is able to communicate with humans.

Smart factory is flexible, homing system which creates monitoring by itself and plans the production according the needs. Smart factory can that way save capital by removing human work, minimalizing commodity and resources. When the system faces faults, it self-directs the bottle-necks and re-plan the production.

Smart factory enables fast go-to market with products and it responses to growing customer needs. Before it has been really difficult to plan smaller production series but now it is possible to tailor production without insane rise of costs and timing. This leads to the concept that the value chain controls itself. Human still manages the factory but no human intervention is needed with smaller decisions in productions or resource management. (Saarelainen & Collin, 2016)

In smaller scale, smart factory and its flexible production can be implemented with 3D printers, laser cutters, and CNC machine tools. With big factories, smart capabilities have already been adapted mostly before with expensive SCADA systems, but now processor power is increasing so they are powerful enough to handle real-time streams from different devices and make analytics. (Bruner, 2013) The factory equipment and software is a mix with different kind of technologies and vendors participating in it. Thus, the factory is working together with all of its elements.

2.4 Industrial internet architecture

There is two ways approach the architecture of industrial internet; the architecture of implementation and the architecture of industrial internet solution. In this thesis, the solution approach is gone through more specifically than the implementation. It is important to understand the solution and layers of architecture before considering information security aspect. The architecture of the solution is based on the system level and technology platform. Architecture presented can be generalized what the industrial internet and even the IoT basically is.

Connected products require companies to build a technology infrastructure (Porter & Heppelmann, 2015). Infrastructure simplifies how the data moves and refines through the technology layers. Basically, the architecture tells how the data is altered to information and that way to business understanding and digital services. Before business understanding and digital services there are no industrial internet, because in that point company is only able to sell their products which compounds different stakeholders (Saarelainen & Collin, 2016).

General IoT architecture consists three different layers; sensing layer, service and cloud layer and application layer (Industrial Internet Consortium, 2015). In Industrial Internet Reference architecture (Industrial Internet Consortium, 2015) these layers in the same order are called; edge tier, platform tier and enterprise tier. The infrastructure is made up with multiple layers of technology. At bottom level, it includes products, their hardware, embedded software, connectivity. In the cloud level, there is data management, servers, analytics and integrations with business software systems. (Juhanko et al., 2015)

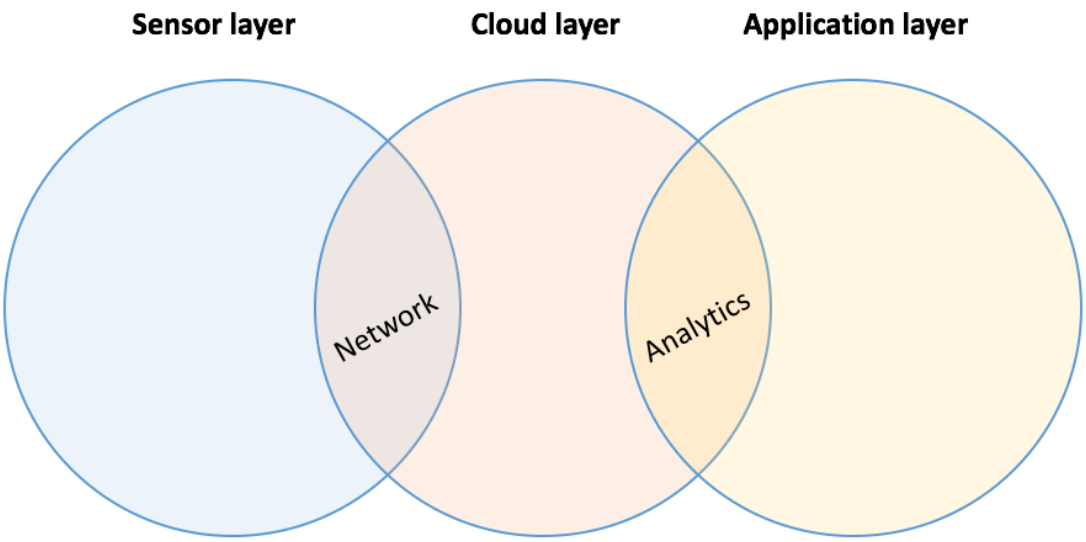


Figure 8. *Simplified IoT infrastructure*

Figure 8 presents the three layers of industrial internet infrastructure. These layers play plays certain roles in processing data flows. Data flow is connected with all of the layers. These layers basically are created when known Industrial Control Systems, the physical layer is brought online with broader systems. The physical layer often is applied with low-latency, fine grained systems without a connection to other systems. In order to control all these systems together remotely centralized data management and operations are needed. Physical systems are directly applied with the operations technology without trying to create any further information from the sent sensor data. IIRA (Industrial Internet Consortium, 2015) also represents that the industrial internet is actually conjoining the two different kind of domains, IT and OT, with traditionally two different kind of purposes and standards together. This actually demonstrates that physical systems (sensor layer) and the functional IT systems (cloud and application layer) can be seen as two ensembles coupled together. But when we are analysing the infrastructure from technical point of view, instead of operational point of view, three layers can be formed.

Generally, technology and the infrastructure is not the bottleneck of creating industrial internet applications, but for understanding what industrial internet means, it is good to divide into smaller pieces. Also, many of the problems implementing industrial internet are between the technological levels. When going deeper from the Figure 8 a technology stack can be presented in more detailed. When exploring the phases of data, at the perception layer nature of the information is data. In this layer networks and sensors are creating the technology. At network layer nature of the information is information, it means that the sensor data is refined in understandable for. At the network layer analytics and data storage is taken place as a technology. At the application layer the information has business understanding and meaning. At this phase sensor data is a value-adding service which allows new services and business. Concrete outcome of the application layer is digital services and different kind of applications.

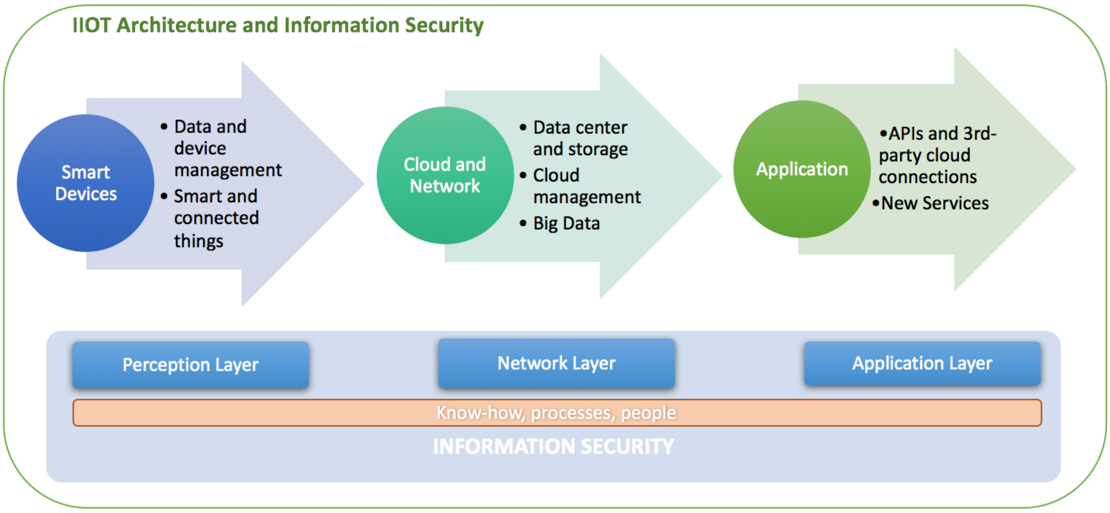


Figure 9. *IOT Architecture*

The challenge of the infrastructure is how to manage the whole technology stack. In order to get the new services and business, the infrastructure should be working bottom up. Different service providers and technologies are implemented, figure 10 gives an example about the players at the IoT technology market. Big IT companies offers ease managing the whole infrastructure with different kind of IoT platforms. Those platforms are like a glue between technologies which enables data collecting, management and analytics. The challenge with infrastructure is also with existing IT-systems (e.g. ERP, CRM) and implementing those into the IoT infrastructure. In many cases the old systems creates a grounding information with the new business opportunities, that's why implementing these systems well is important.

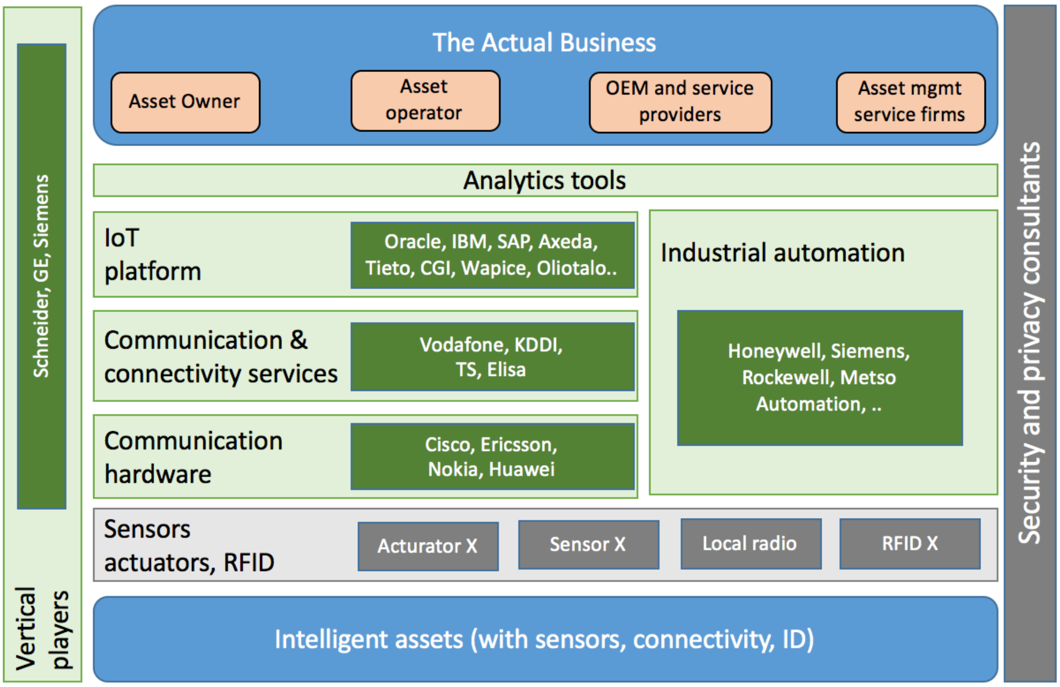


Figure 10. *The players at IoT infrastructure (Ailisto, 2015)*

When there are many different kind of players at the market and companies have to co-operate with many different kind of technologies and implementations. Companies does not implement the whole infrastructure at once. Technologies are implemented step by step. Porter and Heppelmann (Porter & Heppelmann, 2014) introduces that technology stack can be implemented with four simple steps:

- Monitoring,
- Control
- Optimization
- Autonomy

These steps look really familiar with maturity model introduced at Figure 9. But each of these steps builds on the preceding one. For example, if you want to have control capability, first you have to have monitoring technology.

At the monitoring step sensors and different kind of external data sources are enabled. Monitoring can be sensing condition of the products or external environment, but also collecting operational data of the physical element. Product includes its own simple hardware and software to alert ja notify. Next stage control includes software within the product or product cloud to control the product and user personalization. At the optimization phase algorithms to optimize the use and operate the product are included. This is the way to gain product performance and run predictive maintenance. When all these three steps are implemented autonomous operations can be implemented. Ultimately, all products can function complete autonomy and products can have self-diagnosis and service.

2.4.1 Perception layer

In this research prober clarification of the technological stack is started from the machine-to-machine connections and according Porter and Heppelmann’s technological steps towards high maturity of connected products. Perception layer is one of the three tiers introduced by Industrial Internet Reference Architecture (Industrial Internet Consortium, 2015). At that research perception layer is mentioned as an Edge Tier. At this layer data is collected with different sensors and transformed using communication networks. Sensors actually are not a new invention. Before sensors were tailored for use of its target and the sensors were connected to circuit boards which contained embedded software. The IoT trend is to remove embedded intelligence from the sensors and get the physical systems out from local control to remote and autonomous operations. In the other hand, local processing of data is gaining importance. This is because when the processing is done near the sensor, the need of communications network is not that big and the data is more accessible in the cloud layer. (Saarelainen & Collin, 2016)

At this layer two important factors have to be considered. There are various types data so seamless way to produce and transfer data forwards is required. And the other factor is selecting proper sensors by type and specification. (Porter & Heppelmann, 2014) The increasing volume and fall of prices of sensors actually is one of the main source of industrial internet beginning. Normally sensors are included in a variety of devices and solutions. Standard devices collect data from one kind of sensors for example location via GPS, but trend is moving towards multi-sensor elements which contains different kind on sensing capabilities.

Sensor network

Most of the sensors are passive so they just receive information. Active sensors convey energy to environment by themselves and are waiting for response e.g. receiving radio signals (Saarelainen & Collin, 2016).

Sensors are at the bottoms of the technology stack. Sensors are electrical little device which collects information from a physical world. Different kind of phenomena collected by the sensor can be physical or chemical circumstance or event. In the IoT solutions, sensor collects data there where it is installed. Sensor itself does not create usable information about its target and the measuring data is usually an analogical signal which is transferred and converted to digital, with analog-to-digital converters. So, the analogical data from sensors is transferred to separate control unit or the sensor have its own control unit. The value is created with the flow of information and understanding and comparing it to the history data. Simplified this layer detects, collects and processes information from sensors and then transits it to the network layer. This layer can have also its own local and short range networks.

Sensor alone does not make measurable results. Like said earlier sensor environment in addition sensors itself are combined usually with analogy to digital converters, data collections units (Saarelainen & Collin, 2016). If sensor does have its own control unit there might also be software to filter and simplify the data collected from the sensors. Usually this type of set includes also some kind of power source, memory and transceivers. This kind of set is called as a sensor node. Like in Figure 11 can be seen sensor unit usually is made up with four basic components; sensing unit, power unit, a processing unit and a transceiver. Sensing unit usually contains two elements; sensors and above-mentioned analog to digital converters. After sensor data is transformed to digital in ADC it is sent to processing unit. Processor unit will make the sensor data compatible with other sensor nodes and achieve expected requirements of the sensor node. Transceiver connects node to the network. Power unit gives needed power to node. Many sensing tasks require information about the location and even the sensor node can be transferred. That's why in Figure 11 There is locations finding system and mobilizer shown. (Akyildiz, 2002)

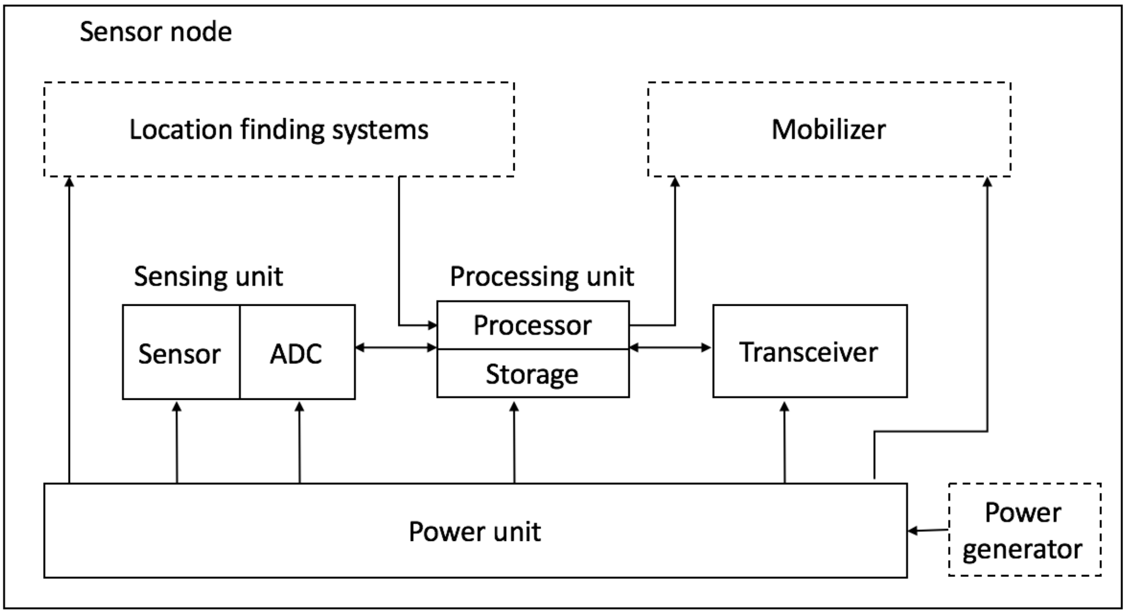


Figure 11. *Components of sensor node (Akyildiz, 2002)*

Power unit is important because the power consumption plays an important role in sensor node. Sensor node can contain energy gathering elements like solar cells and even from environment temperature differences, but usually sensors get their energy from a battery. Sensors power consumption is negligibly small and can be equipped with a limited power source, and sensor node lifetime is in a strong dependence on battery lifetime. That is why power conversation and management take an importance and many researchers are focusing how to invent different kind of power-aware protocols and algorithms (Akyildiz, 2002). All this technology is packed in smaller phase than a match box or even the smallest applications are about a cubic centimetre by capacity. Small wireless sensors are going to be most common types of sensors. In this case, the transceiver is the largest consumer of energy. The battery lifetime depends a lot from the type of communications and the amount of transferred data. However, when sensor is connected with local Ethernet network, it can get the energy from Ethernet cable, this technique is known as Power-over-Ethernet. In wireless applications this is not possible, but in the future, it is possible to supply power through the wireless network. This technique is called as a Power over Wi-fi.

Giving an example how sensors work in real life application. Basically, every machine that registers real-time data can be a sensor when it is connected to network and the data is processed. Car's windshield-wiper, a rain sensor is connected to cars own network. (Bruner, 2013) Sensor from the windshield collects data about the infrared light and if there is water on the windshield the light reflects to different directions; the wetter windshield is, the less light it makes for the sensor. This data is transferred now to cars operating systems. The information from that sensor is combined with the GPS sensor which tells the speed of the vehicle. Then the operating system can do its decision about turning the wipes on and on what speed. In IoT applications the information from this sensor node is sent to upper levels of technology stack.

The most common sensor types gather analogical data from physical and chemical changes of environment. Here are some examples what different kind on phenomena can be measured by sensors and what different kind of sensors are out there:

- Movements, like acceleration, speed, position, gyroscope
- Temperature and humidity
- Pressure of gas or liquid, surface level, flow
- Chemical composition or feature
- Vibration
- Resistance, power consumption and other electronical features
- Radiation with visible light, infra-red or ultraviolet light
- Brightness and proximity
- Biometrics (e.g. finger print)
- Volume
- Weather information like wind speed

There are also sensor types which measures magnetic fields and other environmental measures. Sensor are deployed very close or directly inside the environment to be observed. That is why they usually work places where there is no direct contact available, they can work inside a larger machine or even in the bottom of the ocean (Akyildiz, 2002). Combining different kind of sensors, the machine can be controlled in different ways. It is good to remember that a machine and the entity created by them is usually equipped with multiple sensors with variable mission.

Machine-to-machine telecommunications networks

The data produced by the sensor must be transferred for upper levels of IoT infrastructure and the next base is data management level which means that data is transferred to cloud. There is straight way from the sensors to cloud, but challenging is that there are many different kind of technologies and topologies. When there are multiple options to construct the network using different standards or protocols, there must be clear decisions what is the way create the communications (Saarelainen & Collin, 2016). In practise the goals would be to minimize the used technologies, but when the ensembles are big and use of the sensors and environments are different, there are often used many different kinds of technologies. Also, when thinking that there are many factories from different eras implemented, the IoT networks can be really complex and thus they are difficult to control, maintain and coordinate.

New technologies allow different kind of efficient technologies used in IoT communications networks. Gartner's IT Hype Cycle (Fenn, 2011), measured by the Google search activity, presents impressive hype with terms like Wireless Sensor Networks, Machine-to-Macine Communication Services, Wireless Power and Mesh Networks. Basically, this means that IoT technology will be taken place with environment around us and sensor networks are somewhere in the centre of making this possible. When WiFi and 4G wireless Internet access presence is growing the evolution to ubiquitous IoT networks is clear (Gubbi et al., 2012). Wireless networks are wide spreading sharply, because it is so much easier and faster to expand the networks of them. Also decrease of the price of wireless technology accelerates the expansion. Saarelainen (Saarelainen & Collin, 2016) also says that noted perspective in networks is the size and need for change. Integrating capability sensors with different kind of network technologies is important part of taking technological leaps with IoT development.

Few principals should consider while designing a network for the sensors (Akyildiz, 2002):

- Power efficiency is in an important role
- Sensor networks are data-centric
- Data aggregation is useful only when it does not hinder the collaborative effort of sensors
- Attribute based-addressing and location awareness should be deployed (Akyildiz, 2002)

From the technical point of view sensor networks can be divided on general term in wired and wireless networks. These networks can be divided into three different coverage areas. These three technics, which you can see in Figure 12, are telling about the geographical dimensions of the network.

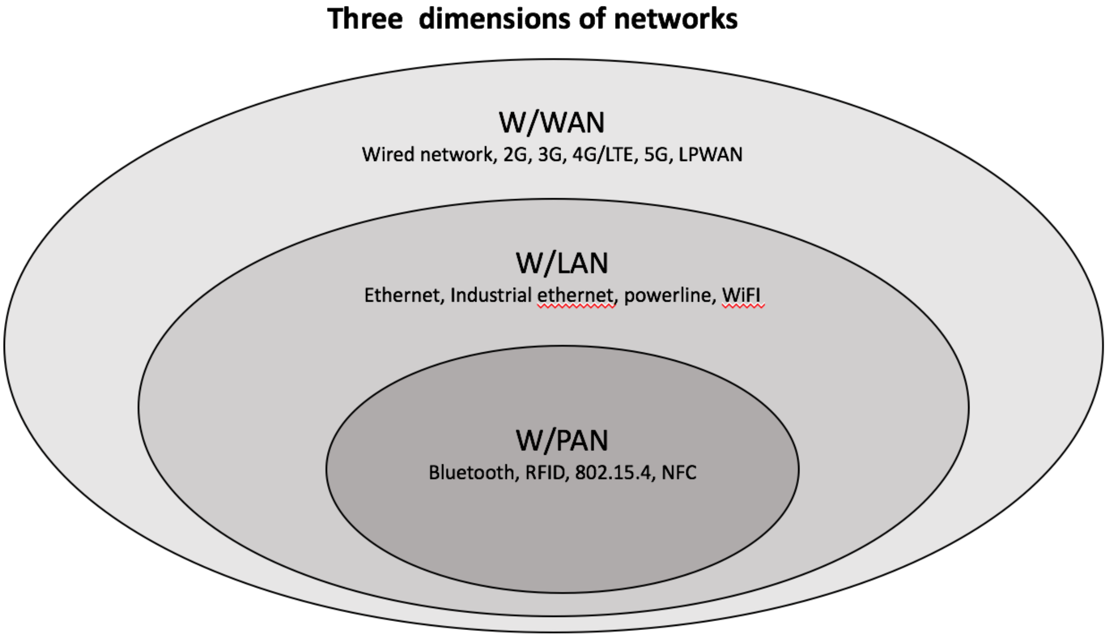


Figure 12. *Three dimensions of networks (Saarelainen & Collin, 2016)*

PAN/WPAN technology (Personal Area Network/Wireless PAN) means personal wireless network, where usually most common terminal is personal smart phone and the most common network technique is Bluetooth (Saarelainen & Collin, 2016). Range of the network is usually from a few meters to one hundred meters and data speed is under one megabit for a second. Despite that PAN networks are called personal, technique is also used in industrial internet applications, where PAN-network is usable in many environments, if there is router nearby. Bluetooth technique requires just little energy. Small Bluetooth Low Energy circuits consumes only a little power and they are really inexpensive. Weakness of the Bluetooth technology is short range and the other weakness is network topology model, where data from the sensors are gathered in one hub (Saarelainen & Collin, 2016). RFID technology was a breakthrough which allows wireless data communication (Gubbi et al., 2012). RFID means radio frequency identification and it allows individual identifications with radio signal. That is how it enables every machine to have their own identity which is formed differently than ip-based identification. Rfid-technology is suitable for use that big number of pieces goes through observation points, this is why this technology is used in logistics and warehouses. Nfc (near-field communications) technology is wireless radio technology similar with Rfid. Signal range is only few centimetres and that's why there is no big IoT applications. 802.15.4 radio standards are suitable with building automation, industrial monitoring and application controlling (Saarelainen & Collin, 2016). With that standard, there are three technologies used in industrial internet applications; ZibBee 6LoWPAN and WirelessHART&ISA100.11a. ZigBee specially is the first real standard solution for IoT applications. ZigBee is a wireless language that everyday devices use to connect to another (ZigBee, 2017). ZigBee networks can contain up to 65 000 devices and connecting to network lasts around 30ms.

Maximum range is about 100 meters. Problems with ZigBee is slow communications, connection instability and security vulnerabilities (Saarelainen & Collin, 2016).

LAN/WLAN (Local Area Network/Wireless LAN) is a standard network which can be wired or wireless. Range can usually be hundreds of meters wired and 100 meters' wireless. Industrial Ethernet is specially for industrial devices to connect. Industrial Ethernet is based on the same Ethernet standards and protocols that used in normal Ethernet applications. So, it can be connected with traditional IT world pretty easily. Of course, industrial Ethernet equipment is made for industrial environments and that is why it differs from traditional office equipment. Powerline also known as PLC (Power Line Communications) is transferring data in power lines instead of Ethernet cables. Technique is used widely in energy sector, but can be used also in manufactories and buildings. This is a quick way to create connections there where power supply is installed and where Ethernet is not meaningful to build. WLAN also known as Wi-Fi is fast and based on Ethernet technology. There is more progressive version for Wi-Fi in IoT applications and it is called WiFi HaLow which is developed for IoT and M2M use. Low power consumption and permeability of structures are taken into account. (Saarelainen & Collin, 2016)

WAN/WWAN (Wire Area Network / Wireless WAN) is a wide range network which is also easily known as Internet. This network technique allows really fast communications. Up to hundreds of megabytes in a second. At the centre of this dimensions are 4G and 5G networks. In Finland Tekes (Finnish Funding Agency for Technology and Innovation) support 5G network development in addition with Industrial Internet development (Juhanko et al., 2015). Main goal is to focus to create groundings for business with handling and transferring a lot of information with real-time and uses it with machine-to-machine communications. 4G technology is becoming a strong option with the industrial internet and 5G technology is forecasted to come in use in the year 2020 (Saarelainen & Collin, 2016). Developed standard for IoT use with 4G technologies are LTE-M, NarrowBand IoT (NB-IOT) and NarrowBand LTE (NB-LTE). LTE-M standard is created for machine to machine communications and it is fully compatible with 4G/LTE network. NarrowBand IoT has been specially developed for narrow bandwidth use and is so very low with power consumption. NarrowBand LTE standard is also very low with power consumption but network suppliers are trying to create the technology as cheap as possible. 5G technology is clearly future and it is developed for the growing needs of communications networks with IoT and for overall large data streams. The goal of 5G technology is to offer at least ten-year battery lifetime and offer very short latency time.

Network architecture and topology is also vital part of successful communications between sensors and cloud. Also, this is very important for information security. All the sensor data is not smart to transfer raw from sensors to cloud platform. Separating meaningful data from all data flows collected to send for cloud platform is important. Usually this is handled with creating a gateway-mediated connectivity (Figure 13)

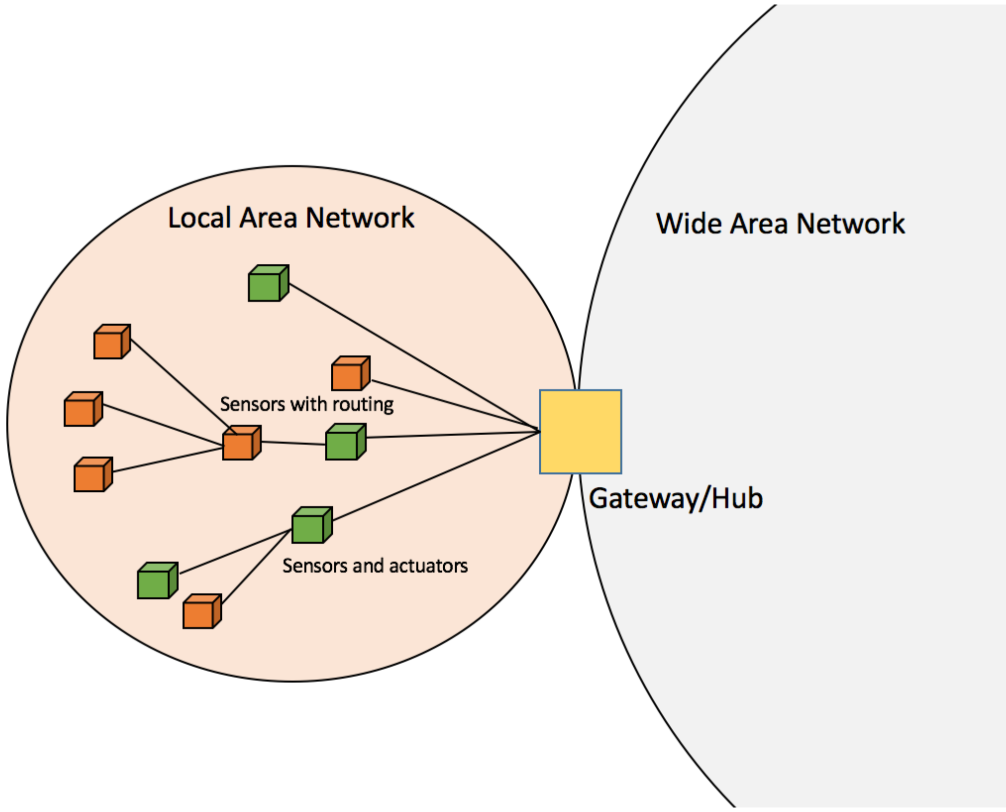


Figure 13. *Gateway-mediated connectivity and pattern (Industrial Internet Consortium, 2015)*

Gateway-mediated network means that local network is centralized to one or more hub before data is transferred further. The gateway acts as an endpoint from wide area network view and isolates the local area network from the outside. This allows localizing some operations and control, usually gateway is a computer and it uses software to filter and analyse sensor data. Gateway enables to reduce communications traffic and act as an integrator with different sensor and actuator technologies used in local area network. The local network can use different topologies. In a hub-and-spoke topology hub has a direct connection with each LAN nodes. In a mesh-network topology hub acts as a cluster for different nodes which can have their own routing capability. This allows sensing layer to be very dynamic. So, sensors usually are not directly accessible from the wide area network. Gateway is an entry point for sensors and provides routing and address translation. Sensor network updates and site-specific decisions can also be done with gateway computer, this allows to do local changes in topology and e.g. add extra sensing technology for the local area network. Then the updates don’t have to strain upper technology layers.

2.4.2 Data management and analytics

Figure 9 shows that data management and analytics happens in network layer. This section was named as data management and analytics because network layer as a nomination can be easily messed up with sensor network layer. Basically, when sensor data is collected together from different sites and sensor count is increasing, sensors cannot be easily anymore managed from the sensing layer. Data volume eventually exceed the threshold that different kind of data storages and analytics platforms may be considered to implement (Industrial Internet Consortium, 2015). Centralized data collection enables to create business adding value when analytics is implemented in top of that. When data is created from different sources, internal and external it is vital to be able to analyse all this data at the same place (Saarelainen & Collin, 2016). The data have to be stored and used intelligently for smart monitoring and actuation; storage, ownership and expiry of the data is becoming important when implementing this phase (Gubbi et al., 2012). Cloud based services and technology means that real-time internet based communications. It usually offers a platform for data storage and service provider software, analytics and applications can be used in top of the storage data (Juhanko et al., 2015). Porter & Heppelmann (2015) refers that sensor data is transferred into product data base. This database enables aggregation, normalization and management of real-time and historical product data. With different kind of integration external information sources (e.g. information about weather, traffic, social media and energy prices) and business systems (e.g. information from ERP, CRM and PLM) is integrated with the database. Storage technology is not a new thing, in the third industrial revolutions when IT was taking place with Industrial Information Systems there were organisations own private storages or data centres. But today when the goal is that the whole supply chain and stakeholders can exploit the value of data and when the cloud storage price has dropped, it is inherent that cloud storage is implemented.

The Jet Propulsion Laboratory has identified some major challenges in data management and analytics (Jones et al., 2012). High volume and low power consumption will create challenges for implementing IoT architectures, machine learning techniques or real-time data analyse and the design of scalable data storages. These challenges guides for more detailed framework how the data management and analytics can be implemented.

Data management

Traditional data management systems normally operate with storage, possible retrieval and updates. In IoT data management, systems are in additional collecting data in real-time, do logging and has to have some kind of facilities for offline analysis (Abu-Elkheir et al., 2013). This expands the concept of data management in IoT systems. IoT can have various number of data sources. The total amount of data generated will grow exponentially and this will set challenges and requirements for IoT data management. The volume of the data is increasing and at the same time verity and velocity is rising. IoT data can include different elements like text, video, audio etc. When the amount of data is increasing, it requires good design from the data storage and management. When scalable data storages are implemented providing efficient data mining and the there has to be a choose where to process data; remotely or locally where the data is stored.

The type of the data storage enables how the data management is scaling. Normally data storages are consisting of databases, but when considering different databases, it should not hinder processing of data, it should make data processing more efficient. Three most used databases are MySQL, Oracle and Microsoft SQL Server (Saarelainen & Collin, 2016). Those all database types follow structured query language, SQL. SQL requires that the data structure is predetermined. With big data masses, normal SQL database is not so scalable and it is getting slower. NoSQL database (non-structural database) is more flexible and scalable than the traditional SQL database. In NoSQL server, different kind of structured and non-structured data (photos, videos, sensor data etc.) can be saved. NoSQL databases are actually a starting point for big data platforms. NoSQL database is a good choice for big IoT database, because IoT data is less or more unstructured and the amount of data is huge.

Big data as term indicated means big mass of data. Most known big data platform is called Hadoop. Hadoop is a decentralized storage system and the server which are creating the cluster. There is a separate disk systems, which split the incoming data around the cluster. IoT will be one of the main sources of big data and the cloud is the place where it is possible to store it and perform complex analyses on it.

In Figure 14 high level cloud architecture can be seen. Firstly, at the bottom of the cloud are the physical storages which are incorporated with different kind of virtual machines. Virtualization is enables physical machine to function as a set of different virtual machines (Buyya et al., 2009). SLA, service level agreement, refers to the properties how the cloud service is delivered for the client. SLA is a set of resource management strategies to personalize the service for example pricing, usage, access and trust.

Data management layer includes lots of integrations. First integration happens when the sensor data is integrated into cloud. This data can be structured or un-structured. But in order to get clear the data there must be integrations to analytics and operations. In the Figure 14, data transform represents different kind of integrations in the data management layer, analytics and when the information is transferred and visualized for the business use. Good to also notice that external data sources need integrations to get effectively integrated with the sensor data at the data management layer.

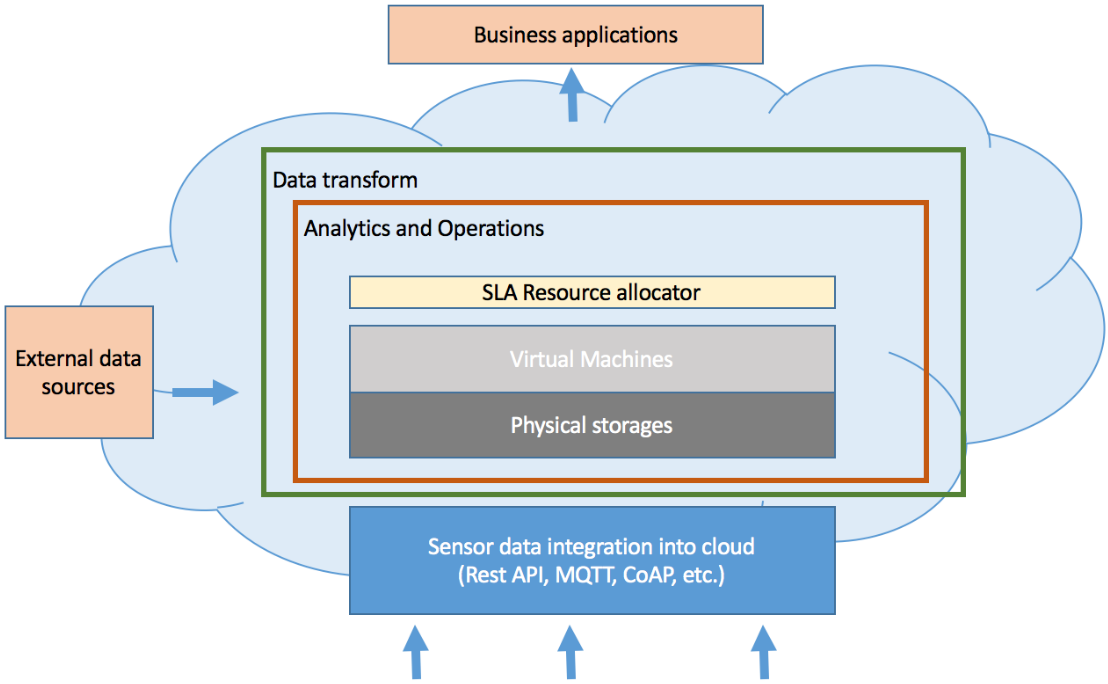


Figure 14. *High level cloud architecture (Chen et al., 2014; Buyya et al., 2009)*

There are different kind of types how the cloud is executed with companies. Cloud computer can be harnessed with SaaS (Software as a service), PaaS (Platform as a service), IaaS (Infrastructure as a service), Public Cloud (storage operated and owned by the company and giving access over a public network), Private Cloud (entitled users only have access for company owned storage) and Hybrid Cloud (private cloud with public cloud access) (Meola, 2016). Choosing the right cloud platform depends of the needs of the company, different kind of attributes can be e.g. integrations, 3rd party accesses, amount of data, analytical capabilities and security. Benefits of cloud technology is low cost storage and automatic scalability for millions different kind of data flows. There are specific cloud services for Industrial Internet which in addition of data storage offers also device management and analytical tools (Saarelainen & Collin, 2016).

Data storage architecture is also a crucial part how to management different kind of data flows. Basically, there are two options; centralized or distributed architecture. Centralized architecture collects data into one background system where all the device management and centralized services are built. In this architecture end points are not in direct contact with each other. In this architecture device management, integrations and analytics are take place from one place. But when the IoT architecture is growing and developing distributed architecture will be introduced when end points are enabled to connect with each other. This allows that some of the processing can be done without burdening the main system and latency is minimalized when some actions are happened near the end points. (Saarelainen & Collin, 2016)

Analytics

Analytics answers to the question what kind of information supports the company's decision-making process and bring value to the business. There are three types of data to generate; history data, real-time data and predictions. Analytics is a model to find patterns from the history and real-time data and use them to make predictions or actions. Analytics can be implemented as from simple rule-based decision making to artificial intelligence. It was mentioned earlier, there can be decision making processes already close to sensors. Those can be set to operate in order fine-tune machines automatically. When talking about the analytics we are focusing intelligence above the data management level. Even if there are some processing power near the sensor, all the data, alarms and communications are happening through the analytics platform.

Analytics is not a process that companies just implement into their IoT project and then it is giving results. Analytics is more like learning path. Companies can test hypotheses with it and slowly learn the systematic analytics after iterating and combined it with external data (Saarelainen & Collin, 2016). IoT stakeholders says (Dimensional Research, 2015) that challenges in data analysis is that there is too much data to analyse effectively and the analysis capabilities are not flexible enough to analyse effectively. Secondly, in acting on analysis IoT stakeholders have recognized these challenges; data is analysed too slowly to be actionable, we're not sure questions to ask and business processes are too rigid to allow us to act on the analysis (Dimensional Research, 2015). Analytics seems to lack the effectiveness to make more meaningful and faster decisions with IoT analytics.

Analytics can be implemented in various levels by its difficulty and know-how. The base for analytics is creating algorithms. Data scientists and analysts might have to code algorithms by themselves using e.g. R, MapReduce or Python programming languages (Saarelainen & Collin, 2016). Today there are also commercial tools straight to implement into use using different kind of cloud IoT platforms. Focus from the programming skills is moving towards asking the right kind of business questions from the analytics. Still analytics is lacking the shortage of talent to take advantage out of big data. McKinsey predicts (Manyika et al., 2011) that United States alone will face shortage of 140,000 to 190,000 people with analytical skills by 2018 and also there will be 1.5 million managers without knowledge and understanding the capabilities of big data analytics.

Analytics can be implemented in different kind of algorithms and level of difficulty. From easier analytics to difficult, analytics can be divided into four different kind of levels (Attick, 2016):

1. Rule-based decision making
2. Statistical reasoning
3. Machine learning
4. Artificial intelligence

Rule-based decision making and statistical reasoning is something that every programmer can do. Rule-based reasoning is used e.g. in notifications, alarms and simple pattern matching. It can be put into service using Boolean algorithms. Ruled-based decision making is more descriptive analytics, it tells what happened, gives alarms and reports. Statistical reasoning uses numerical data and does simple regression. With statistical reasoning, predictive maintenance, data mining and extra- and interpolation can be done and it is more like diagnostic analytics. Rule-based decision making and statistical reasoning can be done by normal programmer. Machine learning goes deep into predictive analytics; it gives forecasts and simulations. In machine learning arbitrary data is abstracted into numbers; relevant features can be identified from large amount of data and the use of different kind of quality controls. Machine learning is usually contributed by data scientists, but there could be also more complex implementations which needs different kind of specialists. Machine learning means basically that machines can learn automatically from their environment and themselves, this allows them to automatically to predict. Artificial intelligence is autonomous selection of best methodology when presented with arbitrary data. Artificial intelligence optimises and plans how to do tasks; it can have human-like conversational skills and think like a digital assistant. Machine learning and artificial intelligence needs big amounts of data to work correctly. (Saarelainen & Collin, 2016; Attick, 2016)

Industrial internet analytics gives integration for the business applications. Also, company can use their existing tools to visualize the analytics data. Many of today's applications includes different kind of dashboards, with good visualization applications IoT analytics can also be more descriptive.

2.4.3 Application layer

IoT architecture (Figure 9) describes that application layer is formed by 3rd party cloud connections and APIs (Application programming interface). These can be created when the whole technology stack is created under it. In this application layer, stakeholders can measure out the benefits of the industrial internet implementation. Applications represents different collection of functions which are reflected to certain business functions. Simplified, application layer provides global management of the application based on the information produced in the cloud layer and analytics (Khan et al., 2012). With applications stakeholders are able to do high level optimization and decisions. Individual machine controlling is mostly happened already at the lower level of industrial internet architecture. Industry applications can be for example management of fleet of devices. IoT also can help to monitor the environmental performance and process data to identify machines that need maintenance (Khan et al., 2012).

IIRA (Industrial Internet Consortium, 2015) refers that application domain is divided into two pieces:

- **Logic** and **rules** are set of variations which are creating the construct and content for the applications.
- **APIs** and **UI** presents the interfaces of the applications. With APIs relevant data is collected and UI is interaction between human and application.

The new business is created when these applications are combined with existing business applications like ERP, CRM, etc. This way the industrial company enables end-to-end operations from the business applications to Industrial Internet System (Industrial Internet Consortium, 2015). The business layer is responsible for the management of Industrial Internet and it build business models, graphs and flowcharts. Based on that information future actions and business strategies are determined.

With Industrial Internet applications masses are not reached. This is because many of the IoT devices are created e.g. for the consumer business. Then there are many users for the applications, but Industrial Internet applications are used mainly by the companies themselves and defined stakeholders (Lueth, 2015).

When creating applications for Industrial Internet, modern agile software development models are introduced. This is the place where small software development company methods are implemented. This means that the basic waterfall model of the software development is not working when pioneering applications are produced. Fail fast -mentality and minimum viable product -method is implemented. With this development stiff and big industrial companies should mutate into agile software houses. Co-operating with 3rd party software developers is vital and the cultural change can happen.

Applications and the business support they are creating are actually bonding the Industrial Internet System with business. In this phase, new business models and services are created. This means that customers can have additional ways of using the products, e.g. pay-per-use and manufacturer can offer additional services like predictive maintenance. Services should be always targeted with certain user groups by their profile, use and pricing. There are many thing manufacturing companies have to consider while creating different kind of applications and services. Seppälä et. al. (Seppälä et al., 2014) presents that digital services includes four basic features which are introduced in following table:

Table 3. *Features of Industrial Internet application (Seppälä et al., 2014; Saarelainen & Collin, 2016)*

Feature	Explanation
Real-time operation	This means that collected data can be analysed and change into meaningful information in real-time. With old-dated information it is impossible to make good business decisions.

Predictability	With analytics and machine learning companies can perform predictive maintenance and environmental changes. Digital services should be able to predictive different kind of changes.
Mobility	Mobility is basically a starting point for all the digital applications today. People are accustomed for using mobile devices and services. Mobility allows to use industrial internet applications from all over the world any time.
Automation	One of the Industrial Internet System goal is that there are ways to make smoother processes and delete manual work. Automation improves the efficiency of processes.

Finding unique added value from the industrial internet systems is the main thing that creates competitive advantage. Well created applications can also shape the organisational culture and business model. This comes when the company is changing into more diverse and agile business environment. Also, there are people with different kind of background involved into projects and development. Manufacturing companies should always thing how to make this kind of switch in the culture for their advantage.

3. INDUSTRIAL INTERNET INFORMATION SECURITY RISK ANALYSIS AND MITIGATION METHODS

When industrial systems are connected into IP world, it means that new kind of threats are established. Aalto University research about open industrial devices found in Shodan tells its brutal story (Tiilikainen & Manner, 2013). Shodan is an online search for devices which are open to outside. The research found almost three thousand open devices. In the third industrial revolution, these kinds of concerns were not important because the devices where not connected to outside world. But now those same old systems are connected to networks and the information security concerns are not considered.

Information security should be implemented and planned together with the other IoT development. All security work starts from the understand of own networks and devices. Factories can be stacked with different kind of networks and layers of technology. Also, different stakeholders e.g. clients are unlikely to adopt different industrial internet solutions if the security, confidentiality, authentications and privacy are not guaranteed.

3.1 Information security goals

Like said, there are huge number of different kind of active or passive devices included in industrial internet system. Information security has been before more about computer systems, software applications and IT infrastructure, now there are devices and plant included. The information security beyond company lines, because different kind of interfaces are offered for the stakeholders. This is why sealing the whole systems is not suitable. Hacker are trying to find open and unprotected devices, after that they are trying to go through the authentication layer by inventing username and password. The other way is to get to read or manipulate control commands. This is possible when unencrypted communication is used. Also, hackers are trying to use the security vulnerabilities of the network devices like routers and firewalls. (Telekom, 2016)

Industrial Internet Reference Architecture (Industrial Internet Consortium, 2015) introduces that information security must be appointed as an end-to-end process. In this operational system both information technology, operational technology and their subsystems must be secured and also situation awareness should be implemented. In order to build a comprehensive security for industrial internet system, these are the main approaches (Industrial Internet Consortium, 2015):

- Endpoint security
- Communication security

- Management and monitoring of the security
- Data distribution and secure storage

Babar et. al. (Babar et al., 2010) appointed that in order to tackle security, privacy and trust in devices and with information high level IoT security requirements are following:

- Secure storage
- Tamper resistant
- Secure s/w execution
- Secure content
- Secure network access
- Availability
- Secure data communications
- Identity management

These approaches are more specifically opened when security architecture is investigated.

Some general components must be implemented when thinking about the overall information security in companies' industrial internet architecture. Miorandi et. al. (Miorandi et al., 2012) have identified three key issues which are represented in Figure 15.

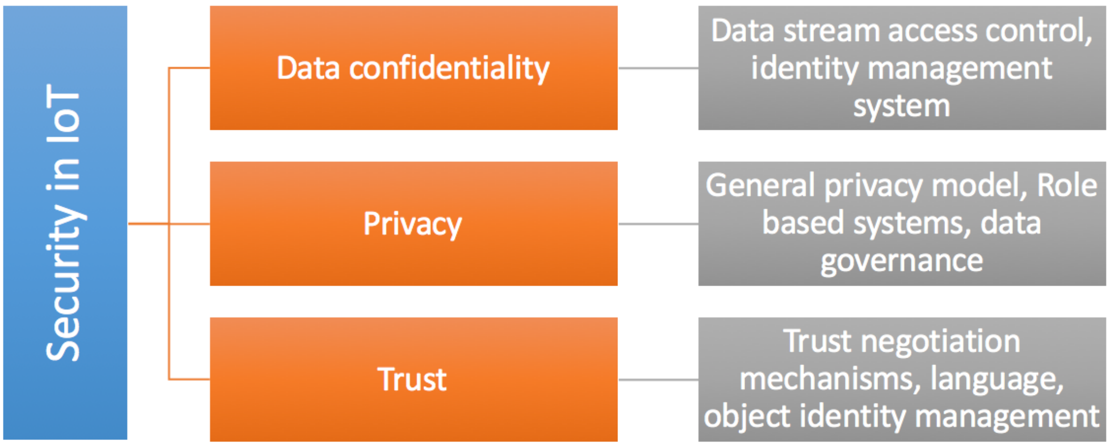


Figure 15. *Security challenges in IoT (Miorandi et al., 2012)*

Data confidentiality means that authorized entitles and accesses are guaranteed. This is important because data can include business confidential information. Defining an access control mechanism helps to keep track about the users. Data confidentiality is also considered when 3rd party data streams are implemented into own applications and big data (Miorandi et al., 2012). So, confidentiality guarantees that information is not disclosed to unauthorized stakeholders. The purpose of confidentiality is to ensure that data transfer between nodes is not accessed or understood by any other party. This kind of confidentiality is usually achieved by access and identity systems, but more specifically using key cryptography where sender and receiver are using a shared key. Confidentiality should be also an autonomic process, because a big deal of the events is happened automatically (Mamoon & Habaebi, 2015). Data integrity is also a part of data confidentiality. Integrity means inability of modification of information somewhere in data transfer. This can be prevented by using cryptography and checksum or message integrity code.

Privacy defines the rules how the data is accessed and shown for the users. Privacy in this context should not be mixed with European General Data Protection Regulation (GDPR) (European Comission, 2015) which means how the personal data is processes and stored. In Industrial internet applications, personal data is not usually stored. Of course, this is something to consider in consumer IoT applications, but it is outside of this research scope. In the IoT systems it is important that information privacy goals are achieved. This can be fulfilled with e.g. with different kind of technologies which enables secure use of data or data provider is able to observe how and what different users are using the system and data (Weber, 2010). Many of these privacy challenges only are suitable in the application level of industrial internet architecture. Privacy is mainly defined in very high level of abstraction; this is because privacy can be different in different kind of systems. Privacy guarantees how the users are able to see the data; is it somehow limited or blocked. In the other hand, it is important that in the systems different users are not able to see how the other users are using the data (Mamoon & Habaebi, 2015). Wireless channels increase the risk of violating privacy e.g. by eavesdropping and masking attacks. This is regulated by the law when personal data is collected, but in the industrial environments privacy is taking into account when thinking corporate espionage and frauds. Privacy is defined by generated privacy models and enforcements models. Also, it should be taken into account what information and to whom it is shown for the users (Miorandi et al., 2012).

Trust is the third security challenge according the Figure 15. It also has many different definitions and it is understood depending on the context. Trust refers to the process where required service is allowed from party to another with obtaining the service. It can be explained like a maintenance of technologies like mobile network is offered to consumers; it relies on working the communications between peers. Many of the trust requirements are met with a reliable identity management and access control, where users can straight get from application to the IoT domain (Miorandi et al., 2012). In this kind of environment where there are many stakeholders included, trust is of course met by beliefs, delegation, credentials, recommendation and reputation (Babar et al., 2010). Babar et. al. (Babar et al., 2010) has also pointed this issues with the proposed security model for IoT (Figure 16).

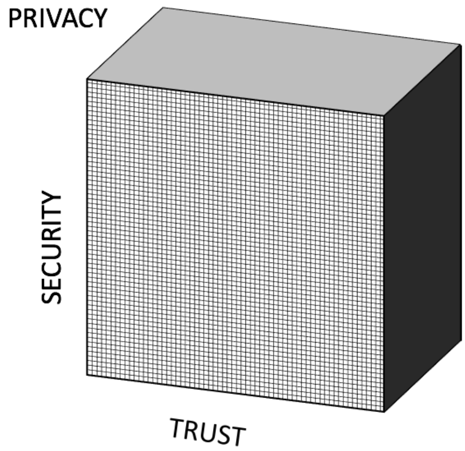


Figure 16. *Security framework for IoT*

These three dimensions of the cube shows the intersection. Privacy includes laws, ethical, user privacy, owner privacy and respondent privacy. Security therefore includes authorisation, identification and authentication, confidentiality, integrity, non-repudiation and availability. The cube describes the high level of interconnectedness between things, services and people. Every information and access in the IoT architecture should be address via privacy, security and trust. (Babar et al., 2010)

Industrial Internet architecture exposes a lot of surface for malicious attacks. Attack surface are physical layer with devices and electronics, but human, network and software (Cam-Winget, Sadeghi, & Jin, 2016). When the IoT system get larger, attack surface also increases and it will be harder to maintain. The technology is developing all the time and new ways of communications and systems are invented. This sets challenges to reach the goals with information security when old technology and structures are mixed with old ones.

3.2 Industrial Internet security architecture

Like presented before, IoT primarily operates on three layers which are perception, network and application layer. Each layer of IoT has inherent security issues due the technologies used. In this section information security threats, techniques and technologies are presented in relation to the IoT architecture. Some of the threats and techniques can be repeated in different layers, so it is smart to clarify threats compared to IoT architecture. Threat taxonomy is presented in Figure 17. The list of the threats and measures to tackle these threats are described more specifically when going deeper to the security architecture in this chapter.

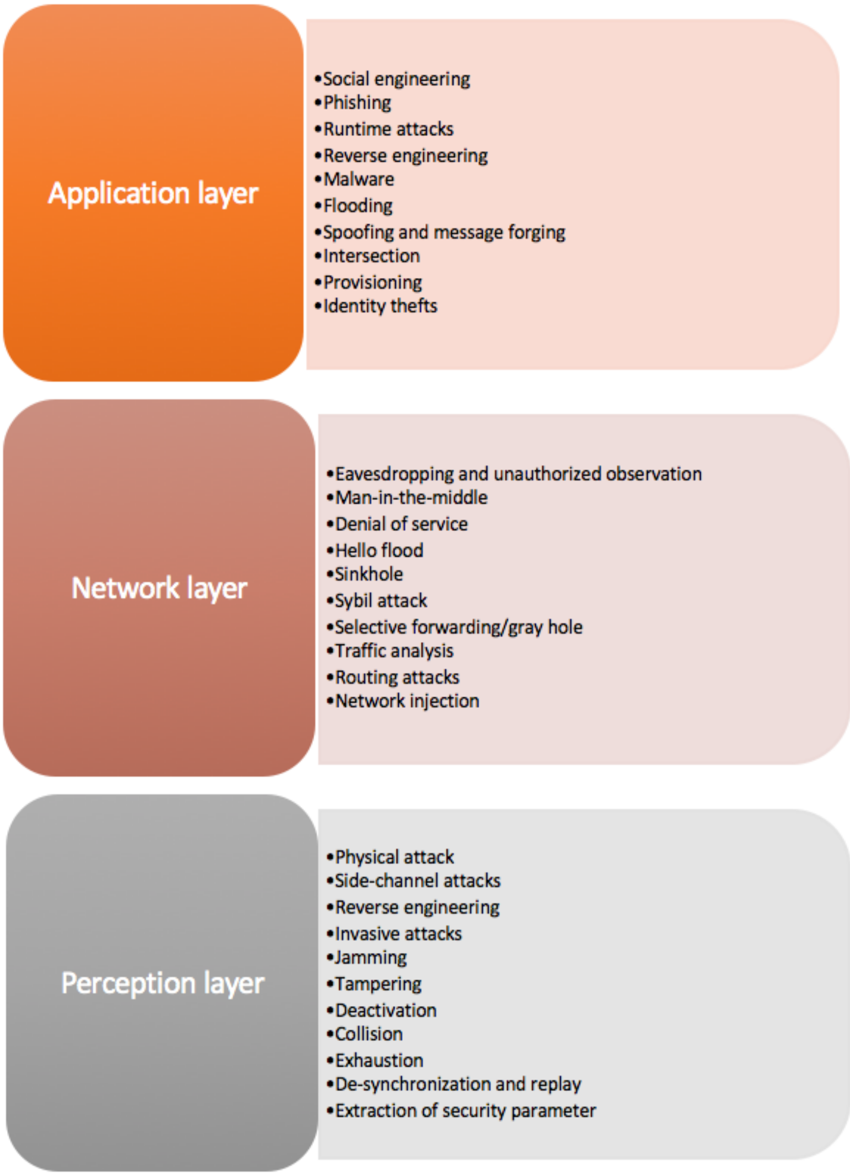


Figure 17. *IoT architecture threat taxonomy. (Mamoon & Habaebi, 2015; Babar et al., 2010; Mahalle et al., 2013)*

In the other hand security challenges of the IoT can be also broadly divided into two classes; technological and security challenges (Yousuf et al., 2015). Technological challenges are related to wireless technologies, scalability, energy and distribution of IoT. Security challenges are in this breakdown considered as the challenges related to security services like authentication, privacy, trustworthiness, end-to-end security etc. This is good to remember while planning the security for the IoT. The security is not only about the security services and technologies, security in the IoT is also about the used IoT technologies and the architecture of the whole system. For example, where the memory and processing is taken place, which wireless connections is used and how the technology stacked is scaled between the layers and other devices. Also, Ashraf et. al. (Mamoon & Habaebi, 2015) describes that security constraints are higher at the perception layer and are getting lower in higher levels of the architecture.

3.2.1 Perception and network layer security

In industrial internet applications, the biggest attack surface is in perception layer. There can be huge amounts of different kind of devices and networks, which can be geographically remote. Complex is also that some of the devices can be old and are usually tried to implement as cheaply as possible. Also, many of the IoT devices do not have appropriate user interfaces and communications to pair with the older technologies.

International Journal for Information Security Research (Yousuf et al., 2015) describes that there are three main security issues in IoT perception layer; strength of wireless signals, physical attacks and dynamic IoT topology. Signals are usually transmitted in perception layer via sensor nodes used different kind of wireless technologies and it can be compromised by using disturbing methods like different radio frequencies. Sensors are microprocessors are also prone for physical attacks because they are usually external and located outdoor environments and attacker can tamper the hardware components of the device. Data tampering occurs when attacker modifies, adds or erases data from the end device. This happened when node is physically captured from the network. Attacker can be able to reprogram, redeploy and recover devices when the attacker has studied the type and format of the data transferred in IoT devices. Tampering can be prevented with autonomic scenes for self-protecting and device authentication. But also, a hardware design of the device and secured physical design can give tampering resistance. (Industrial Internet Consortium, 2015; Mamoon & Habaebi, 2015) In addition to tamper-resistant hardware and device authentication, sensor networks must be created resilient. This can be done e.g. with resilient routing protocols and then the system is able to work even if some of the nodes are under malicious attack (Chan & Perrig, 2003). Attackers can also obtain their own commodity sensor nodes and include the network accept their additional nodes. When attackers have control of some nodes they can easily distort sensor data, extract private information and even enable denial of service.

Jamming is one of the usual attack types in the perception layer. Jamming based attacks are really high threat in IoT because devices are usually remote and connected wireless. Jamming means that radio frequencies are disturbed by use of interference or saturated with other signals which are effecting to the right signals (Mamoon & Habaebi, 2015). Jamming can be mitigated and prevented by proper monitoring; sniffing details about the wireless information and changes. Jamming the channels can cause Denial of Service (DoS), when the wireless communications network is under targeted attack e.g. by jamming the channels (Roman et al., 2013). Exhaustion and collision are really close to jamming. In collision, the attacker forecasts message transfer timing and then the attacker sends the message at the same time with the right message and it will result the collision of the message. In bigger infrastructure, simultaneous attack messages can cause random harm, when the message collides with random packet transfers (Mamoon & Habaebi, 2015). Collision can be prevented and noted same way than jamming, but autonomic system recovery of the systems can variable packet timings and help to prevent further damage. Exhaustion means that many of the sensor layer node power are dependent on long life batteries. When the sensors are attacked by mentioned ways it will exhaust the batteries, because attack prevent mechanisms have caused a lot activity and stress for the sensors. Use of cognitive adaptions and use of timers and limitations will enable also with availability.

Deactivation of the sensor means that it is taken away by some malicious application or physical attack. Sensor can be found and destroyed or attacker will try to find a way for the interface. This can be prevented roughly by password protection or using camouflage. It is not so easy to recover from the physical attacks, but if the deactivation is done by application, node can be restored by commands (Mamoon & Habaebi, 2015). Controlling also means taking over an IoT device and after the attacker can do desired vandalism with it. In these cases, it is important to have a proper monitoring for the IoT devices, which alerts about lost nodes and performs self-healing processes. In this kind of monitoring, if the system identifies any kind of suspicious traffic in the sensor it may instruct to delete any information from the microprocessors and what is stored in the device. This will also help that it cannot be reverse-engineered. Reverse-engineering means that by investing the device you are able to understand the logic of the device and use the information against the system.

In de-synchronization and replay attacker will collect the transferred data and then sent it repeatedly for the end-point. Replay attack is also one of the easiest attacks to perform. Many authentication systems are immune for this kind of attack, but it can be easily prevented by encryption of the messages with dynamically changing session key. (Mamoon & Habaebi, 2015)

In wireless sensor networks, attacker can have an access to private sensor information by monitoring node transfers (Chan & Perrig, 2003). This is called eavesdropping, but also can be called node capture. Eavesdropping can happen in various communication channels, like wireless networks, local networks and Internet, sot it is not just a threat in perception layer. Eavesdropping is really easy to execute by internal attacker who is able to access the infrastructure (Roman et al. , 2013). External eavesdropping can be prevented by encrypting sensors, with end-to-end encryption.

DoS attack is often mentioned when talking about attacks to IoT devices. DoS attacks can exhaust the service provider network bandwidth and other resources. In DoS attack, attacker can take control part of the infrastructure physically or disturb it other ways e.g. by manipulation and delays. DoS attack can also occur inside of the sensor network if attackers can compromise sensor nodes. Then attackers can e.g. create routing loops which eventually exhaust part of the infrastructure. DoS attack can be prevented by the techniques that are also used towards other kind of attacks at the perception layer. This can be e.g. spread-spectrum communications and frequency hopping towards jamming, authentication so any message cannot be accepted. Message authentication can be built by using e.g. signatures based on asymmetric cryptography so the protocol itself cannot be energy exhausted. (Mamoon & Habaebi, 2015; Roman et al. , 2013)

As mentioned, large number of IoT devices exposes the system for attacks. First thing to prevent these from happening is to ensure the basic security of the software, infrastructures, applications and computer systems. Companies must know what devices and software there is and how they are connected. Also, it is important to understand what kind of information is. Then company can create a risk overview from their IoT devices. Used devices, communications technology and techniques should be measured in order to find old devices and techniques prone to attacks. Hardening for the devices and networks should also be done; adding extra layers of security, switch default passwords, authentications etc.

IoT systems are created by using components from multiple vendors and with different levels of security. In order to create security to this kind of technology stack, it must be built by design rather than bring it in afterwards. To create security by design it requires a precise overview about endpoints, communications, endpoint management and data storing. This must be always analysed towards cost aspects, future implementations and development, security functions and possible customer requirements. Endpoint security actually is a lot dependent on the interface they expose. Many of the security functions can be implemented to work autonomous to accomplish required security policies. As we went through earlier, there are many different ways to attack to endpoints, so there has to be also many ways to secure the endpoints. For the endpoint security IIRA (Industrial Internet Consortium, 2015) list for endpoint security is applied present.

Secure boot attestation means that a prescribed sequence of steps is used to restart endpoint from a known secure state. If the endpoint boot sequence is altered, security agent should be able to stop or guarantee the endpoint. Security agent can be either process-, container-, virtualization- or gateway-based. Process-based security agent means similar agent operations as anti-virus application are working. Container-based security agent can be implement straight to the endpoint including some storage and software. Virtualization-based security agent can gain visibility of the bigger environment that just one endpoint due virtualization. Thus, it is able to control multiple security activities like embedded identity, secure boot attestation, communications etc. Gateway-based security agent is physically really close to device and is used in the cases when security cannot be embedded for the device. Then gateway-based security agent itself takes role in security functions. (Industrial Internet Consortium, 2015)

Every endpoint must have a unique identity so they can be managed and tracked. Endpoint has unique identities e.g. IP address or MAC address, but they can be easily altered it they are not secured. Created unique identity code can be secured by given credentials.

This kind of credentials can be gain by using cryptographic keys which are secured by the hardware.

When the endpoint is attacked, it should defend itself and also be able to report the attack further and reconfigure itself. The same security management system which is able remotely and automatically update endpoint, should be able to gain the knowledge about the endpoint attack. It is important than when one endpoint is attacked, other endpoints cannot be compromised. In order to recognize the attack, endpoint must work together with security monitoring and its analysis. When attack is recognized, security monitoring and management system should reduce the risk and bring the system back to the steady state according the policy. Policy is embedded with the central security management system and it is spread for the use of security agents. (Industrial Internet Consortium, 2015)

Security monitoring should also gain information about the events occurring at the endpoint like updates, log in/out information, violation and authentications. When log management is done, all the information should be also stored. In the fear of possible attacks, log management information should also be stored in secure location like cloud and not only locally. (Industrial Internet Consortium, 2015)

There should be also mechanisms at the endpoints that only authorized applications and networks so any other is not able to connect directly with the device. This is called whitelisting. From the security management system, it should be able to change the policy about whitelisted networks and applications. Opposite whitelisting is blacklisting, it means that security policy has set some applications or networks not to contact. All these attempts and connections collects information for the log management system. (Industrial Internet Consortium, 2015)

When inspecting more deeper communications between the devices there are more things to consider that just technology. E.g. how to build network topology and architecture which prevent possible attacks spreading and multiply. Weak network topology is a possible source for security vulnerability. Attacker can also try to create false routes, and the data is transferred through bad route e.g. through attackers own device. (Lu, 2014) The devices are connected with each other directly or through gateways and there might be also great heterogeneity between different technologies. This poses challenges of maintain communications between devices. In the IoT architecture there can be devices from different organizations. This sets challenges and attributes from the network access management. Also, the performance of the network should be considered before setting up security protocols; network latency and throughput should be at the good level (Industrial Internet Consortium, 2015). In the creation of the network architectures, it is good to consider which layers and parts to protect and how to protect them.

When devices are creating connections between each other at the perception layer, two-way authentication can be implemented. This way sending device can ensure that the information is not only sent to the device which is receiving the data. It is also good to consider that communications type and what data record to share with who and under what condition.

One thing what is highlighted, in addition to device authentication, is encryption. Data exchange between endpoints must be encrypted with cryptographic keys. In Encryption, key management is important to create effective and agile. Good encryption mechanisms ensure good data integrity and it determines who can see the data (Khan et al., 2012).

Network visibility is one other key thing in IoT systems. Monitoring and diagnostics are vital to minimize and prevent the downtime (Evans & Annunziata, 2012). In monitoring, there are closely set algorithms to identify problems and changes according to history data and set limit rates. Thus, it is easily possible to connect two critical systems of IoT; monitoring and cyber security management. System is able to collect real time data and offer the architecture; parameters can be also monitor data structure, encryption, transfer mechanisms and the proper use of data (Evans & Annunziata, 2012). In addition to single event monitoring and alerts there should be trancing for emerging threats through the history data and sequences. E.g. if there is a single port scan event, it is not interesting, but if there is series of port scan it might be a sign for a system wide attack (Industrial Internet Consortium, 2015).

3.2.2 Cloud layer security

This layer like described is responsible for the service management and has a link to database (Khan et al., 2012). It receives and collects information from the network and store it in the database. All these operations of course must comply with privacy regulations and still performance operations through data analysis (Industrial Internet Consortium, 2015). Industrial Internet Reference Architecture (Industrial Internet Consortium, 2015) describes four consideration shown in Table 4.

Table 4. *Data distribution and storage security considerations (Industrial Internet Consortium, 2015)*

Security consideration	**Description**
Data security	This means encryption of the distributed data in all circumstances. Access control to the sensitive data should be enforced with authentication, authorization and control policy.
Data centric policies	This includes security requirements and policies like data security, privacy, integrity and ownership in all stages. This is set by industry standards and laws, e.g.

	how to collect and file automotive information or vital parameters in a nuclear reactor.
Data analysis and privacy	Provide data access policy to enforce fine-grained data access rules. E.g. what information from the data records can be distributed with the 3rd parties.
IT systems and the cloud	Data storages are detached from the industrial system so provenance information and privacy requirements should be attached with the data. This helps to maintain the knowledge of ownership and custody chain.

Like mentioned previously, the link between IT world and physical devices are done by interfaces. A secure basis for all traffic to and from the cloud platform is Transport Layer Security (TLS) encryption protocol or Secure Socket Layer (SSL) protocol. This is part of the end-to-end security and mitigates many kind of risks all over the IoT system. (Telekom, 2016)

Main threats in cloud layer are flooding, malware, spoofing and message forging and intersection. Flooding means exhausting of the important resources by sending many connection establishment requests. This can be easily mitigated by setting up connection establishment barriers for autonomic self-protection measures. Malware attacks confidentiality of information. Malware may not affect sensors, but can exist for gateways being presented as applications in the mobile phones. So, infected mobile phone may show application look-a-like authentication interface for the systems, but is really a malicious software. Mitigation for malware usually includes vulnerability scans and risk mitigation services. Spoofing means that attacker impersonates sensor node and it is noticed as a valid node. This way attacker can insert wrong kind of information for the system, message forging also includes forwarding existing message with different content. These kinds of attacks can be mitigated with autonomic manner and encryption. In intersection attack, the goal is to defeat the privacy of the system by focusing on the auxiliary information of the system. Attacker tries to get the privacy information model by collecting data from different sources (e.g. web, 3rd party records) and link them to create understanding of the systems. (Mamoon & Habaebi, 2015) This threat can be mitigates using e.g. k-anonymity (Sweeney, 2002).

Responsibility of the cloud layer attacks is a difficult to define. Cloud service providers are responsible for providing secure and standardized interactions, interfaces and storage. The steps between machine network and cloud can be attractive attack target. So, the implementations and cloud service provider selection should be done carefully. At this point a central surveillance authority might be required to define and monitor security policies, authorizations and authentication mechanisms. Cloud service providers can prove their security by certificating it with information safety management systems, e.g. fulfilling ISO/IEC 27001 requirements. This way IoT systems owner can rely for the cloud provider.

Responsible by the service provider is usually described in a service level agreement (SLA). Service level agreement defines customer needs, provides framework, reduce areas of conflict, eliminates unrealistic expectations and it is simple a list of promises how the cloud service is offered for the customer. Service level agreement discusses also how the security is maintained, what methods are used how customer communication is taken care (Kandukuri, 2009). From security point of view service level agreement should discuss at least following issues:

Table 5. *Security considerations in service level agreement (Kandukuri, 2009)*

Security issue	Description
Privileged user access	Information about the people who manage and have an access to data.
Regulatory compliance	Service provider offer proof or willingness to perform external audits and security certifications.
Data location	Which country data is stored and how they obey local privacy regulations.
Data segregation	Evidence about encryption schemes are designed and tested by experience specialists.
Recovery	How backups are set up and where. And what is the post-disaster strategy.
Investigative support	Support for the investigation requests in case of inappropriate or illegal activity.
Long-term viability	What is the process in case of bankruptcy or acquisition.

3.2.3 Application layer security

In application layer security issues can differ a lot between the applications and systems. This is because, there is no standard application which is used in this layer. Application layer security is complex. In this part application layer security is approached by Zhao et. al. sum of some common security problems (Zhao & Ge, 2013) in Table 6 and Open Web

Application Security Project approach of application threat modelling and awareness for web application security (OWASP, 2017).

Table 6. *Common security problems in application layer (Zhao & Ge, 2013)*

Application security problem	Description
Data access permissions and identity authentication	Effective authentication technology should be implemented, with spam/malicious information processing.
Data protection and recovery	User privacy and data loss mechanisms.
The ability of dealing with mass-data.	If data processing can't meet with the requirements and needs of data flow, it might lead to network interruption and data loss.
Software vulnerabilities	Software and code is not developed to meet security standards and expectations.

The Open Web Application Security Project (OWASP) is a worldwide non-profit organisation focused on improving software security. OWASP gives articles, methodologies, documentation, tools and technology for application security. OWASP methodologies are in common use among information security professionals, when web application security tasks are conducted. In this research, it is not necessary to explore very it very precisely, but top risks and preventing should be explored. Application security is important because, attackers can use many different paths through application to do harm. Every potential bath is representing risk for getting hands into lower levels of technology and information in IoT architecture. In IoT systems there are usually many applications implemented, so it is important to shut all possible paths for exploit, or at least make it difficult. OWASP top ten most critical web applications security risks and preventions are described below top down: (OWASP, 2017; OWASP, 2013)

1. **Injection** means sending untrusted data e.g. SQL command to the system and the system can that way execute unintended commands. This can be prevented by using safe API or whitelisting the inputs.
2. **Broken Authentication and Session Management** means that attacker can compromise passwords, keys or session tokens or exposing other identities. This can be prevented by using a single set of strong authentication and session management control

3. **Cross-site Scripting (XSS)** occurs when application takes untrusted data and send it to a web browser without proper validation. Preventing this threat requires separation control from untrusted data to active browser content e.g. with white-listing inputs or using auto-sanitization libraries.
4. **Insecure Direct Object References** occurs when developer exposes way to get internal implementation object like file or directory. This can be prevented by using indirect object references and access control checks.
5. **Security misconfiguration** means that good security configurations are conducted with application, framework, web server, database server and platform. And also, the configurations are updated regularly when needed.
6. **Sensitive Data Exposure** poses information for attackers e.g. credit cards and personal information. This kind of exposure is mitigated using cryptography for all sensitive data with strong key management and avoiding storing unnecessary personal data.
7. **Missing Function Level Access Control** is happened when the identification is for the application is going to happen. Different access levels for the service is given according the credentials, attackers are able to forge different level access controls if the control checks are not safely created. This kind of control check can be created by authorization module.
8. **Cross-site Request Forgery** forces to send logged users cookies and authentication information. This allow attacker to force victim's browser to generate requests the vulnerability application thinks are legitimate requests from the victim.
9. **Using Components with Known Vulnerabilities.** These components can be such as libraries, frameworks and software modules. Attack can cause data loss and server takeover. This can be prevented by updated software components, in some cases security can be increased by added security wrappers, monitoring components and established security policies.
10. **Invalidated Redirects and Forwards** to other pages and websites which can be phishing or malware sites. This can be prevented by avoiding redirecting sites or involving destination parameters to ensure validity of supplier. (OWASP, 2013)

In industrial internet systems, many of the applications are used through mobile user interface. Mobile security is therefore one of the security issues also. Of course, when developing a mobile application, there are many similar threats that with a normal web based application. Mobile security should enable ubiquitous and easy access to IoT data while providing control and security. It is also good to consider that mobile device monitoring and control does not use the personal information of mobile user. Mobile security the simplest is already presented device identification, authentication, key and credential storage and exchange. (Sicari et al., 2015)

4. RESEARCH METHODS

This empirical part of the research is conducted from the theoretical framework created using literature and other researches of the researched are. There are articles and researches about the IoT security, but answering to the main research questions is hard to find straight answers. IIRA (Industrial Internet Consortium, 2015) research gives as a good insight what is important in securing IoT systems, but does not take a stand where in architecture companies should prioritize the security investments. In Chapter 5. Interviewing results are assembled together and conclusion combines theory and empirical party by offering a model for how information security risks could be prioritized in industrial internet security development. Challenge collecting theoretical framework was that there was not so many extensive researches about Industrial Internet security. The area is still developing and the standardization of the IoT security is not completed.

Like said, theoretical framework was created by using literature review from industrial internet, IoT security and other supporting material. The goal in empirical part is to analyse top business risks and information security risks in industrial internet information security. In order to do this, theoretical framework offers information about industrial internet, its maturity and architecture and what are the security threats and methods of prevention them. Firstly, industrial internet theory was presented and on that architecture, security aspects were added. Theory was conducted by using big number of different kind of articles. Difficulty creating comprehensive theory was that most of the articles took stand generally on Internet of Things. Industrial Internet is only part of the Internet of Things, so choices had to be made in order to just keep the theory around Industrial Internet. E.g. privacy related things were not studied in such detail, because priori personal information is not collected from industrial internet systems. In theoretical framework, many security related details were simplified. This research should give an overall review about how to secure industrial internet system, now how to do it precisely. This research should be able to read by people which have basic knowledge from the researched are, not by people who wants details. E.g. there are many different kind of wireless communications technologies like 3G, Wi-Fi, Bluetooth etc. but it introducing how to secure them precisely is not intended. It is just good to know that there are different kind of technologies and how the wireless communications are generally secured. Some of the literature researches and articles goes really deep into some specific details about certain subjects, e.g. how to secure communications. This complicated the decisions what is relevant to go through in theory and what is not. Also, some of the articles are conducted by using old reference material, what means that some of the details might be old-dated in this fast changing are of application.

Empirical part of the research was realized by arranging unstructured interviews using ***Appendix 1*** as an interview frame. Interview frame was prepared by choosing the themes we want to know in order to answer the research questions. When preparing questions, it was important that they are created in such a manner that it is easy to answer and create conversation. It was important to ask questions which are more general about industrial internet and its security. Detailed questions about industrial internet security would have been hard to answer, because interviews were conducted to management. Delimiting this research for industrial vendor segment was good, because the overall view about industrial internet was the same. But the maturity of the industrial internet represent companies were different and this is what should be taken into account in the results. Also, the scope of industrial internet is big in the companies. Choosing and getting the right people interviewed, which are able to understand the whole picture of industrial internet was difficult. Interviewed people were found through relations and just by searching suitable profiled people from LinkedIN and contacting them directly.

The goal was to interview representatives from eight big industrial vendor companies in Finland. After all, representatives from six different companies were interviewed. In three interviews, there were one person participating, two interviews with two representatives and one with three representatives. All the companies and representatives are going to stay anonymous, because sensitive nature of the subject. Even titles are not exposed in order to keep the privacy. Interview answers were collected by recording the interviews. One interview answers were collected by typing, by interviewees wish. Each company were given a short summary how they answered relative to other companies. In the Table 7 interviewed persons and dates are described.

Table 7. *Persons interviewed for empirical research*

Organisation (code used from now on)	**Responsibilities and number of interviewed persons**	**Interview date**
A1	1 interviewee responsible of industrial internet development	20.10.2016
A2	2 interviewees, responsibilities: - Responsible of automation development and maintenance - Responsible of industrial internet research and technologies	4.11.2016
A3	1 interviewee head of business line with the use of industrial internet technologies	11.11.2016

A4	2 interviewees, responsibilities: - Head of business unit with the use of industrial internet technologies - Responsible of data collection and information management.	18.11.2016
A5	1 interviewee responsible of industrial internet related cybersecurity	22.11.2016
A6	3 interviewees, responsibilities: - Digital Architecture - Information security - OT/IT integrations	5.12.2016

Timeframe for this research was from August 2016 to April 2017. The actual theoretical framework research including getting familiar with the source material in writing the theory took time from September 2016 to February 2017.

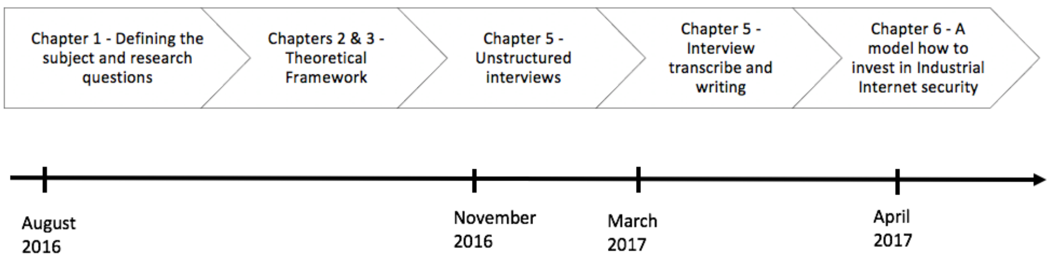


Figure 18. *Phases of the research in relation to time*

5. RESULTS – UNSTUCTURED INTERVIEWS

In this part, interview results are conducted from the interviews and structured by the questions. Questions for semi-structured interviews can be found from Appendix 1.

5.1 Industrial Internet maturity

First interviewers were asked how industrial internet appears in the company and what is the maturity of it. When asking this question, architecture of industrial internet and M2M Maturity model was shown (Figures 5 and 9). Every interviewed company's revenue is calculated in billions, so in Finnish scale they are really big. Every company informs industrial internet to be an important venture and for most of the companies' digitalization is one of the strategic focus points. It is important to understand the maturity and the use of the industrial internet, because with that information this research can offer also a point of view that which cyber risks have been risen on different stages of maturity.

There is not so many differences with maturity model positioning between interviewed companies. In big companies in Finland, devices have been smart for years, even for decades. Third industrial revolution has enabled the use of IT and embedded devices. But there were no open interfaces to public internet and all the data was only used sited itself. Today computing power has increased and sensors has become cheaper, allows more sophisticated use of IT and harnessing the benefits of industrial internet.

In these interviewed companies, there are many different kind of product and business lines. It is clear that the company, as a whole, is not at the same phase of industrial internet maturity at the same time. Also, depending on customer segment how the industrial internet can be implemented. Interviewers mentioned, that some customers do not easily offer interfaces to public internet in order to transfer data. E.g. in maintenance critical environments like in energy business it is difficult to access the data because of the possible risks of doing so.

In M2M Maturity Model (Figure 5) maturity is divided into four steps; smart connection, smart analytics, deep learning and new business. Smart devices have been in use for years and smart analytics has collectively been implemented last years. Overall every company answered that the maturity with their industrial internet is somewhere between smart analytics and deep learning. Maturity of interviewed companies is presented in Figure 19.

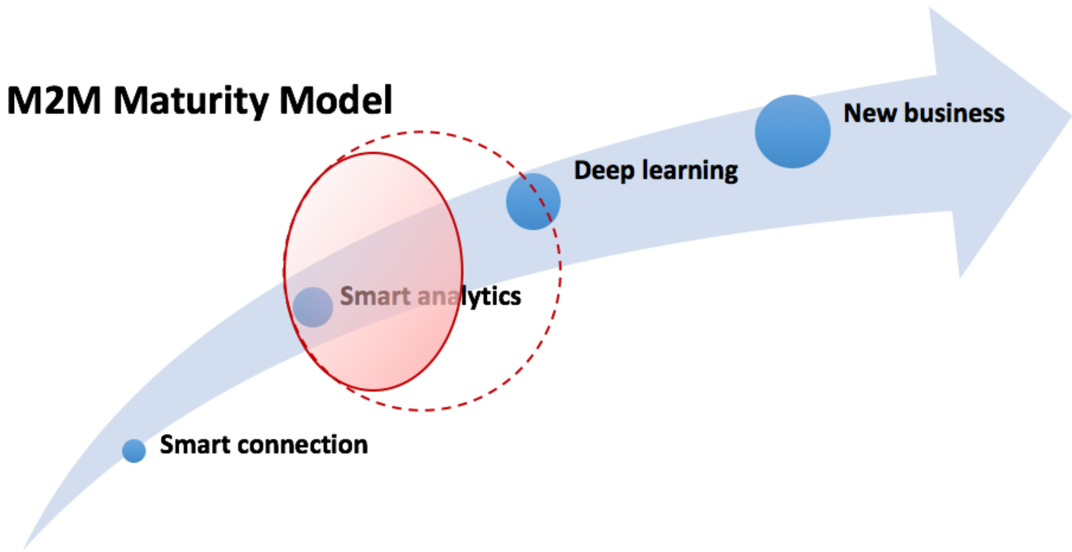


Figure 19. *Maturity in interviewed companies*

All interviewed companies positioned themselves as average or forerunners of the industrial internet maturity in this segment. However, every company said that their maturity is somewhere between smart analytics and deep learning. Some of the products might already be in the stage of deep learning but most of the business is in the level of smart analytics. Respondent A6 seemed to be just a little bit below from the others, saying that they are mostly using smart analytics but not yet everywhere.

Companies have used internal servers for a while, where all the data is collected. This is mainly because this kind of technology has been possible to implement for years. Public clouds for this kind of industry is rather new thing. And before comprehensive big data analytics, public clouds have not brought any benefits for the business. The big change among the interviewed companies is that they are at the moment in a big change from private clouds and servers to public, 3rd party offered cloud services. This is something where are still many question marks and how to implement it efficiently. And private clouds are and are going to be important in critical environments.

New business is also interesting point of view for the industrial vendor companies. The basic outcome is that customers can see their products and their condition through applications. But in some cases, it is not so simple that giving a customer interface to monitor conditions of devices. Some factories can run though day and night, despite the condition of the products they are able to change products only during a planned maintenance outage, which is performed e.g. every five years. In this kind of business, the real values e.g. of predictive maintenance can remain limited. New business can be also tricky, because every industrial site and customer is unique itself, many of the industrial vendor companies of course offer tailored solutions for the customers. This can also be a show stopper for many industrial internet possibilities. In these kind of cases, possible new business kind of systems can be really expensive and it is hard to get value out of them. Common difficulty to harness new business opportunities in industrial internet applications were that the customers are not able to implement new kind of technologies and in some cases, they are not even willing to start talking about giving their information out from the company's firewalls. Also, one thing to consider new business was that if industrial devices are becoming fully automated without human intervention, it can risk the physical safety in factory site.

Industrial internet is a kind of a hype like artificial intelligence and big data at the moment. Many companies do have industrial internet in their strategy, but only small group in the companies understand the possibilities of the industrial internet. So, there is a lot of work to do in the cultural change also.

5.2 Information security risk analysis in industrial internet

5.2.1 Why to invest in information security?

Interviewees were first asked why to invest in information security. After that they were asked if there are so big information security risks which prevents the full use of industrial internet potential. After overall questions, business risk was examined more specifically and they were pointed into the industrial internet architecture.

Question three in the interview dealt with the overall feeling why companies should invest in information security in industrial internet. Reason for asking this question was that we can get an impulsive answer what are the first things what comes in the mind as the biggest considers of the industrial internet security. Answers were pretty similar among the interviewees. After the overall question, more detailed question about business risks was asked in question five.

The overall answer for the question, why to invest in information security in industrial internet system was that always when interfaces from site to public internet is opened, attack surface will grow radically. In this point for securing the production and customer information, it is vital to have this interface secured. This can be compared with physical safety, why there are locks and guards at the office premises? So, when endpoint communication functionality is created between devices and data storage, networks should be segmented, identity and access management, encryption and other protections should work. According the A2 information security should be done correctly right away, it should be implemented already in the planning and architecture. If the information security is not implemented in planning phase, it is really hard to add there afterwards. A1 answered that information security investments should be tolerable. Industrial devices should have basic security implemented, but while the competition is hard in this segment, all the investments which may increase the price of the product or decrease its margin, must be considered carefully. But when talking about individual device, the value of the transferred data should be taken into consideration all the time, because what would attacker do with the data of individual device? But if the attacker is able to get into the bigger system and more comprehensive through the device, it should be taken into account.

One main answer for this question was that with the information security investments and security of the products, companies are able to convince customers and that will gain trust. There is not yet many cyber-attacks in this segment, not that many that it would be a big problem. That is maybe one reason that information security has not been the main issue of the industrial internet development and making the legacy products open to public internet. But there is always a flip side; if the amount of attacks will increase significantly, industrial companies are going to close the interfaces and data communications to outside world, which will be a close call for industrial internet.

It was said that there might be customer demands for information security in order to stay in the race. But also, customers could demand information security to be reflected in some certain standards like ISO27001 or some energy sector standards. At the moment, there are not yet standardized solutions for industrial internet security, but customer can value that product information security is compared with some general standards.

5.2.2 Is information security hampering industrial internet development?

Question four in the interview was that "Is there so significant information security risks that industrial internet cannot be implement as its full potential?". This means that in some phase of industrial internet maturity and development, are the information security risks growing so big that the development cannot be implemented. Answers can be seen below:

Table 8. Answers of the questions related to information security show stoppers

Respondent	Answer
A1	There are not so big risks.
A2	There are no show stopper risks; all the risks should be all recognized and then mitigated. This should be done with every risk.
A3	Yes. Some industrial companies do not want to open interface outside, because they are not familiar with all the risks or do not want to take risks. This affects implementing industrial internet technologies.

A4	No, we are living in society where everything is shared and connected. Information security is always considered and there are technologies to mitigate risks.
A5	Business values goes first, information security follows business decisions.
A6	Not that kind of risks, but the problem is that customers are not willing to open interfaces outside factory sites. But it is not impossible that in the future there might be that kind of cyber-attacks which will affect on this questions also.

According the answers can be assumed that there is not at the moment so big security risks (five out of six respondents answered “no”) that will be affect how well industrial internet can be implemented. However, respondents cannot forecast what the future will bring and if there will be really high risks in cyber security which just cannot be mitigated with known protocols.

5.2.3 Top business risk attached to information security concerns

In the next phase respondents were asked about the main business risks, this means that what is the main business risk or lost they are afraid of cyber security attack is going to happen. They were shown a list of main business risks what would occur from bad information security. They could use it in order to help to answer to this question or they were also free to choose an answer outside of this list. Respondents gave their opinion top three business risks, biggest risk coming as a number one:

Table 9. Top3 business risks in relation to cyber attack

Respondent	Answer
A1	1. Availability 2. Customer data 3. Integrity
A2	1. Availability / interruption of the production 2. Customer compliance

	3. Reputation
A3	1. Availability / interruption of the production 2. Information risk (customer or own data) 3. no answer
A4	1. Availability / interruption of the production 2. Information risk (customer or own data) 3. Reputation
A5	1. Availability / interruption of the production 2. Customer compliance 3. Information risk
A6	1. Information risk 2. Reputation 3. Availability / interruption of the production

Next question (Question 7, Appendix 1) asked respondents to localize business risk to industrial internet architecture. Every business risk was not gone through precisely, but overall feeling where from the architecture would those mentioned business risks occur. Four out of six (A1-A4) respondents answered with one accord that the biggest risk in at the perception layer; including smart devices and connections to the edge of the cloud. A5 answered that it is not so unambiguous to localize risks to certain point of architecture. It is important to constantly parse attack vector and then mitigate risks and build protection. A6 answered that there are two critical ways in order to risky business; get customer information from cloud with some kind of bug or vulnerability, or device will be updated or controlled remotely from cloud or application which will interrupt the production. When roughly highlighted these attack vectors to industrial internet architecture, it will look like this:

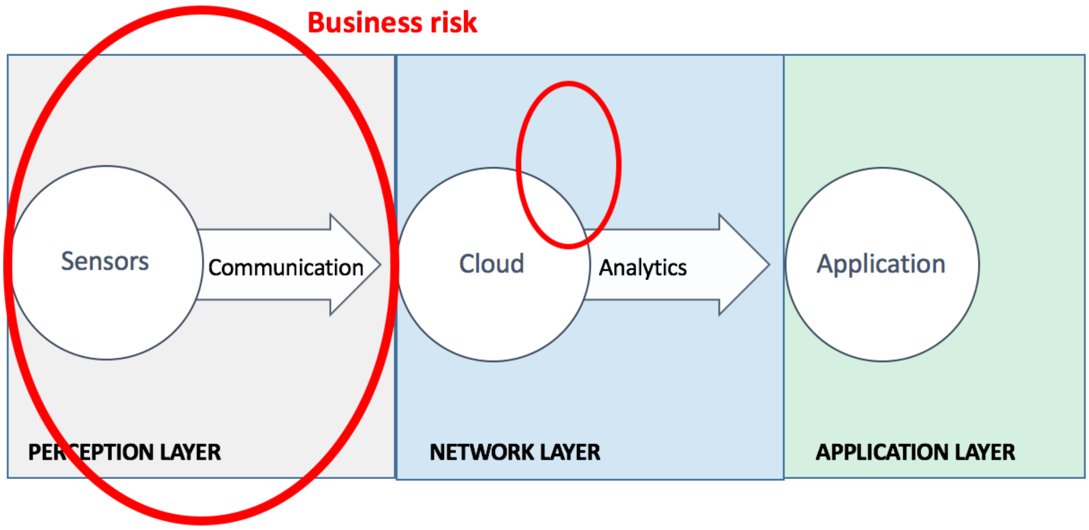


Figure 20. *Business risk focused on IoT architecture*

Even if respondents said that the biggest risks might happen in perception layer, they highlighted still that the biggest single risk for industrial internet security is the user. This means that reason for cyber-attack can be very humane; using infected USB sticks, leaking passwords and phishing attempts.

5.3 Information security risks in industrial internet

Question 8 in interview handled concrete information security risks. Like in business risk related questions, respondents were asked to describe top three information security risks. After arranging the information security risks, respondents were asked to target the risks to the industrial internet architecture.

Table 10. Answers for information security risk question

Respondent	Answer
A1	1. Network vulnerabilities 2. Physical threat 3. Embedded security
A2	1. Identity management 2. Encrypted communications 3. Physical threat

A3	1. Cloud interface vulnerabilities 2. Network vulnerabilities 3. Embedded security
A4	1. Encrypted communications 2. Cloud interface vulnerabilities 3. Identity management
A5	1. Identity management 2. Privacy 3. Mobile security
A6	1. Identity management 2. Embedded security 3. Physical threat

All these information security risks also were positioned to the industrial internet architecture. Information security risks with emphasis can be seen in the following figure:

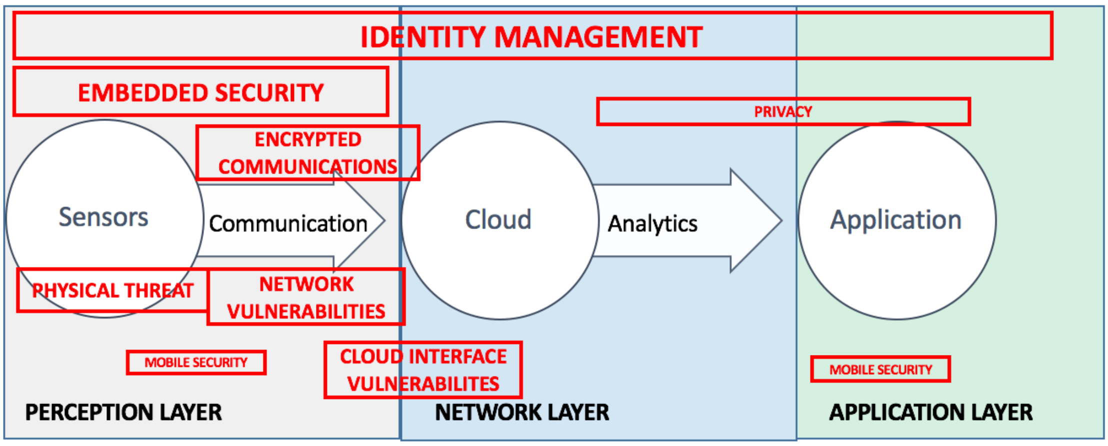


Figure 21. *Answered information security risks pointed out in industrial internet architecture*

When looking at the Figure 21, it can be seen that respondents are highly concerned about perception layer information security risks. Specially communications network between sensor and cloud is something where most of the information security risks can be positioned. This will affect to the model which we will introduce in Section 6.

6. DISCUSSIONS AND CONCLUSIONS

6.1 Discussion

The main findings from the empirical study was that companies are scared interruptions in production and information risk. This basically means that most risk for the companies is in the customer interface. Companies are not afraid losing their own data, but losing customer data from their industrial internet system and applications. Identity management, embedded security and physical threat were the biggest information security risks for interviewed companies. All business risks and information security risks were positioned to perception and network layer of the industrial internet security. This tells that there are wider attack areas, legacy systems and devices and companies may not have full control for the operations in those layers yet.

In the research interviewed companies were first asked why to invest in information security. After that they were asked if there are so big information security risks which prevents the full use of industrial internet potential. After overall questions, business risk was examined more specifically and they were pointed into the industrial internet architecture.

Also, it was good to notice that companies are not exactly innovating the industrial internet security approaches. They know that for every problem there are already solutions available. If companies need to e.g. add some extra encryption on their industrial internet communications, they can do the research and implement already known technologies. Information security is implemented step by step using already known technologies. This approach has worked.

In empirical part interviewees were asked more generally that as an industrial vendor, in what are information security investments are especially important. Response was generally that of course companies must pay attention for the weakest points of the system. This kind of work happens all the time in companies and information security work is continuing. All thought when thinking about original information security, it usually means governance risk and IT security. Industrial Internet brings its special perspective with smart devices and stakeholder participation. This is why usually the information security work is focused for the perception layer.

In the interviews, there were also small discussions about the liabilities in industrial internet technologies. This is good questions, because there are lot of service providers including building the industrial internet system. According respondents, responsibilities are usually done dynamically with subcontractors and service providers. With the service providers, a comprehensive valuation must be created in order to answer the questions;

are they a secure partner and is their operational model suitable for the company in legal point of view. Responsibilities are created always case-by-case, but someone has to take the total responsibility and usually it is the industrial vendor; but of course, cloud provider is responsible of their SLA and application partner is responsible that secure code is delivered.

The last question of the questionnaire was about asking risk management methods for the top three information security risks. This question was generally hard to understand and answers were very variated. As a conclusion, there are lot of different kind of models, guidelines and certifications were to compare own information security work, but there is no standardized way for industrial internet yet. Some customer may ask about the certifications, but e.g. ISO 27001 certification is a huge work for the company and it can create really heavy processes for the company. But still, these kinds of guidelines must be taken into account in order to meet the customer compliance demands. It is important that industrial vendor company understand their status of information security work and works according the prevailing situation. For this work also affect the detail that is there common goal for information security work or is it just an active process in action.

6.2 Conclusions

Industrial internet, as a part of Internet of Things, is going to be a big change in industrial and manufacturing world. Drivers towards the change are considerable, when it is technologically possible and big companies are setting the digitalization in their strategies. But there is the "but" behind the hype; cyber security. It is easy to become a cybercriminal and earn reasonably well. There are plenty of examples how factories and sites has been attacked with very sophisticated ways. Industrial companies compete in global markets where product cost is tuned to its peak. The fear of the cyber-attacks is present, but at the same time companies might lack the skills and resources how to mitigate cyber threats. This thesis collected information about industrial internet and its maturity, after that a theoretical framework of industrial internet cyber security was combined from today's articles and researches. In empirical part, big Finnish industrial vendor companies and their business leaders were interviewed about their visions and feelings about the cyber security of industrial internet. As a result, top business risks and information security risks was conducted and they were positioned to the industrial internet architecture. All the appropriate information was combined and rough model how to approach cyber security in Finnish industrial vendor companies was introduced.

Original motivation to do this research was that there is no standardized model how to approach information security in industrial internet system. There are huge threats when smart devices are connected to the internet (Saarelainen & Collin, 2016), but at the same time there are lack of information security knowledge in business lead and that's why resources are not allocated for that work. One of the biggest industrial internet advocate in Finland, former-CEO of Konecranes Pekka Lundmark, has said (Lehto, 2015) that industrial internet will success or fall for cyber security. There is a contradict for this all hype and this research was done to understand what it most important in cyber security in industrial internet companies.

Research question 1, RQ1, "*What are industrial internet information security risks and how they should be mitigated in Finnish industrial vendor segment?"* is answered pretty widely in the research. Theoretical framework gives a basis for this question by analysing overall risks for industrial internet information security. In this chapter, 6.3. Recommendations, more generalized model for this question is conducted. "Research questions RQ1, RQ2 and RQ3 were well answered. For the research questions RQ2, "*What kind of information security risks appears in different levels of industrial internet architecture?",* and RQ3 "*Why is it important to invest in industrial internet cyber in industrial vendor segment?",* results were basically mostly answered in theoretical framework. For the RQ3 there was also results in the empirical state. Research question RQ4, "*What is the role of industrial vendor company in industrial internet information security?",* was not answered so clearly. Some theoretical framework and empirical results referred for this question. But also like said in empirical results, all the responsibilities with 3rd party providers are always negotiated case by case and agreements and SLAs are created." Subquestions (SQ1 and SQ2) are more supportive questions to parse theoretical framework, these questions are answered in theoretical framework.

6.3 Recommendations

In section 5 empirical study to Finnish industrial vendor sector companies was executed, and results about information security in industrial internet was found. Research Question 1 (RQ1) asked that: *How industrial internet security should be approached in Finnish industrial vendor segment?* This section will compile results for that main research question. In theoretical framework, there was lot of information security threats and mitigations introduced, but it did not take stand what is relevant and in what order for securing the industrial internet.

In this research, the companies under investigation have already start their Industrial Internet journey. Mostly have smart devices with some kind of connections, some have already created very sophisticated methods to collect and use the data in their system. When creating a guideline how to invest into industrial internet security, it should be also taken into account that there are still machines that are not connected into the industrial internet system. Like seen in Figure 19 interviewed companies' maturity level is smart analytics and in some cases or business units' deep analytics. We can assume that there are some kind of communications already created.

Respondents described in interviews that if information security becomes hard and complicated it will not get implemented. Manufacturing today is very agile and it always finds a cost-effective way to do things. If information security is complex and expensive, it will not be implemented. Even if information security level is a competitive advantage, industrial vendors compete very price driven market, so the components should not increase the price of the products.

In order to give recommendations for information security work in industrial internet, business risks and information security should be conducted from the Section 5. When business risk answers according Table 9 is conducted, and pointing results as follows; top one risk got 1.5point, number two 1.25 point and number three 1.00 points. When adding these together we can have a table for top business risks:

Figure 22. *Business risks valued from the answer*

Top three business risk were pretty obvious, but when looking deeper those answer, it can be seen that reputation is more like an outcome if cyber-attack happens at it will go public. But as a business risk point of view interruption of production and information risk were the highest. Interruption of production was a risk if it happens in customer premises, it could cause billion scale losses. Also, the information risk was not considered so bad if own device data is stolen, but if through device attacker is able to stole customer data and get hand into their systems. Customer compliance in this case means that company is able to offer products which will meet customer requirements. E.g. in energy sector they can be pretty demanding in specific markets.

It is difficult to analyze severity and probability, because industrial vendor companies are not able to impact them in customer sites. Just hope, that own device is not behind the possible cyber-attacks. But of course, companies are able to give best practices for security and offer services with devices which will possibly improve.

Scoring the information security risks from the Table 10 in the same way with business risks will give following results:

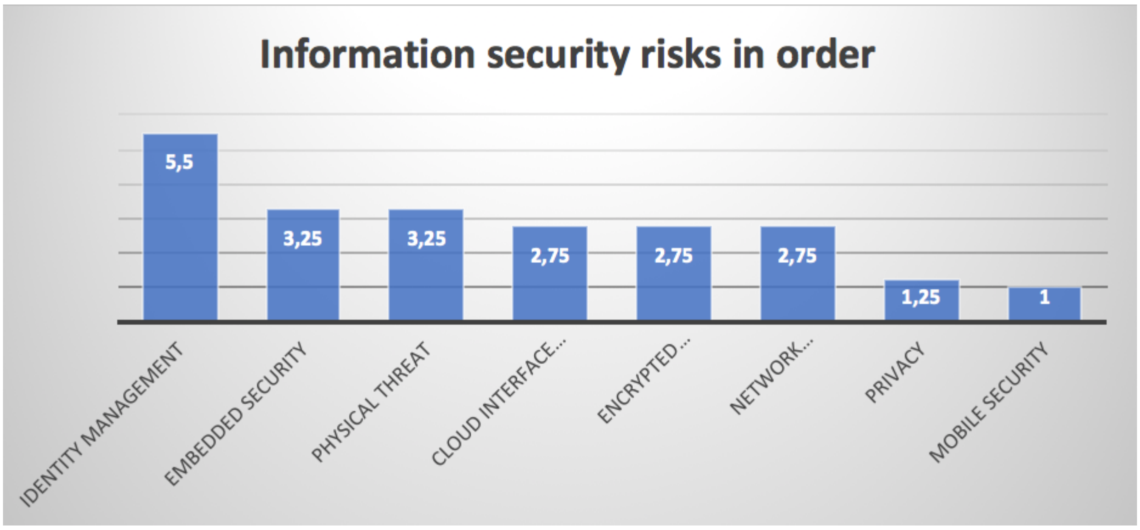


Figure 23. *Information security risks in order according interview answers*

Identity management emerged in many answers and got the highest points. Identity management can be understood both device identifications and user identity management. Together four respondents answered identity management to be one of the top three information security risks. When described in more detail, two of those answers referred to device identities and two to user identification. But overall, identity management is not an unambiguous to understand and we can generalize that identity management is important in many ways in industrial internet systems. Also, when mobile interfaces and communications are becoming more common, device identification is in a key role. Always when e.g. new device appears to the system, it is critical to identify it as a right device. These kind of attack surfaces are all over the industrial internet network. In some customer facilities, there are still old devices in use and thus there is not even possibility to use mobile networks and identifications. Identity management is also important because information is shared with other stakeholders. When there are a lot of external identities in the system, it also set big requirements and protocols from identity and access management.

When checking the interview results from business risk and information security threat point of view, can be concluded that interviewed companies generally are working with the same problems and in the same level in industrial internet architecture. Some companies could have been taken some things into account than other, but security development process of course operates from acknowledged risk point of view. In order to clarify where should the industrial internet security work start potential threats and business impacts should be identified. Carty et. al. (2012) introduced a security investment model where different defence layers in linear fashion prevents malicious attacks.

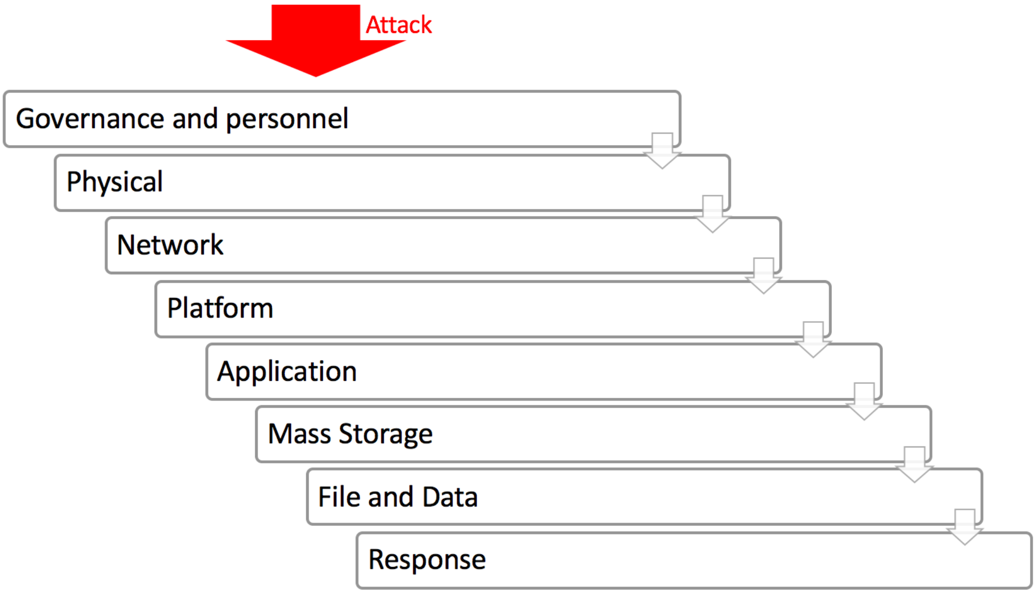


Figure 24. *Layer of defence in information security attacks (Carty et al., 2012)*

These defence layers have been chosen in that order, because it facilitates the calculation of risk and estimation of value of security investments (Carty et al., 2012). At the first step, there is governance and personnel and management of this layer is a quick win in order to mitigate cyber risks. Three of six respondents in interviews pointed that a blue-collar worker around smart devices or application user is the easiest target for cyber-attack. Educating the users and stakeholders can prevent human errors.

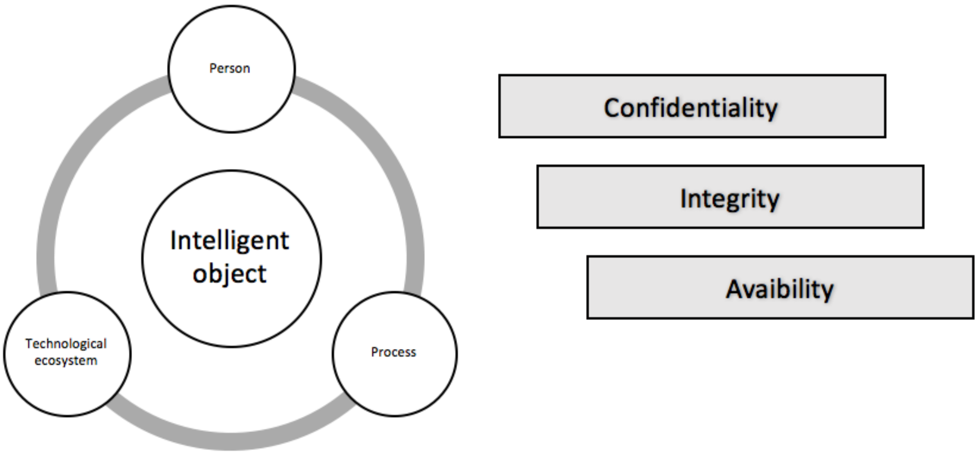


Figure 25. *A systematic approach for IoT security (Riahi et al., 2013) and CIA-model*

Riahi et. al. (2013) introduces a systematic approach for IoT security. This model consists of four different dimensions; person, technological ecosystem, intelligent object and process (Riahi et al., 2013). These four dimensions should be covered when implementing a IoT security process. For the person defined rules, processes and limitations. Process in this means accomplishing tasks in IoT environment according the security requirements. Intelligent object means an object what is capable of communicating with the environment and respond to events. Technological ecosystem refers to technological choices made to ensure the security. Choices can affect in affect in every layer of Industrial Internet architecture. This is something to consider all the time when improving and analyzing Industrial Internet security. CIA-model is something that is generally used as a principal for information security work for organizations, this has already been introduced in section 3.1. In Industrial Internet systems availability rises over confidentiality and integrity, at this can be seen already in the top three business risk in empirical part.

Every development work starts from current status mapping. In industrial internet security, this means identification of potential threats with their possible business impacts. After this it is possible to get an understanding and visibility of potential threats. In section five, respondents already gave a harsh estimate what do they think that are the biggest security threats and positioned them at the Industrial Internet architecture. In section three there was IIRA's list of relevant security concerns (Industrial Internet Consortium, 2015). The list of these relevant security concerns also highlighted endpoint security and communication between the endpoints very vital. These are elements that also aims for data confidentiality and trust (Babar et al., 2010). The security development work should be based on the main business risks, in this case this refers for availability and information risk in perception layer and cloud.

Theoretical framework and empirical results are being combined using the model of layer of defense from Figure 24. From all this information, a model how industrial internet information security can be approached is introduced. The model is presented below, in Figure 26.

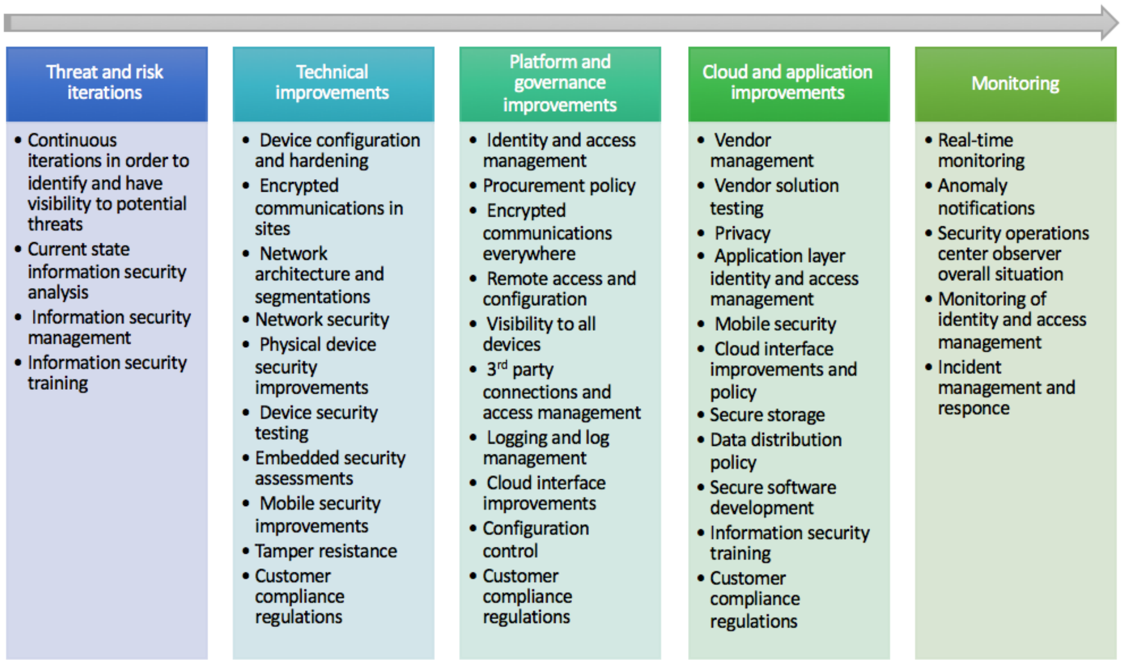


Figure 26. *Proposed model for industrial internet security*

First some kind of roadmap should be created and have an understanding that continuous information security improvement work and management should be done. At the first phase, when industrial internet capabilities are implemented, in information security point of view, there is quick wins with information security training. Industrial internet security plan can be created only when current state is known. Everything what is done for information security should first being planned and compared. This gives understanding how to improve information security. As a conclusion to this phase, it is said that information security should be a continuous process inside the organization.

After the evaluation, technical improvements are conducted. Many of the responded companies have already smart devices in use and many of the improvements of Figure 26 is already noticed and taken into account. Also, it is very difficult to change some features like physical appearance and chosen technologies afterwards. In principle, it is very difficult to overlay information security improvements. But also, there are ways like hardening and network security to taken into account in this section. Network architecture and segmentation is something to improve in this phase. In site premises, it is also important that there is an understanding that the attacker is not able to violate customer security though device or its' network. Device should be implemented with ways of recovery from the disaster. In order to maintain customer production, site end network should be able to work "offline". This means that if there is a cyber-attack, machine or network should notice it and is then able to continue its' process ignoring the attack. Industrial components should be able to work without connections to outside. In this phase, some certifications e.g. Https and TSL can be implemented.

After technical improvements, platform and governance improvements should be implemented. After technical improvements, identity and access management should be implemented in the industrial internet system. This means whitelisting with networks and devices, endpoint identity, access control, logging capabilities and creating a remote police management. Most of the interviewed companies are in this phase according the interview. In this phase, whole network security should be improved from endpoint to endpoint, above all from device to cloud interface. Platform improvements also enables remote access and configurations to the endpoints.

In the next phase cloud and application improvements are done. Of course, technology vendor evaluations are done before, but in this phase, it is important to understand how the data is stored in cloud services and used in applications. Concept how to evaluate security should be implemented when co-operating with 3rd party service providers. Companies should evaluate is it possible at all to co-operate with certain service providers; technological, legal, insurance, SLAs and responsible rule aspects should always be evaluated. Cloud and application security improvements and manners are already discussed in greater detail in sections 3.2.2 and 3.2.3. Interviewed companies did not yet took these aspects as a priority. These security improvements are coming after the industrial internet system is secured in lower layers of industrial internet architecture.

Monitoring is introduced as a last phase of industrial internet security model. Security monitoring gives a real-time snapshot from the industrial internet system. This increases the situation awareness. In concrete, security operations center observes anomalies from industrial internet system. Diagnostics is collected with SIEM (Security information and event management) service. Monitoring collects information from the endpoints, security events, attack attempts, status, health and so on (Industrial Internet Consortium, 2015). Monitoring parameters are basically implemented by the need of the industrial internet system in order to maintain security and predict or notify attacks and changes.

Overall, there are two things to consider when companies are securing the industrial internet system; return of investments in information security improvements and efficiency of the used security strategy and actions. Technical improvements what the competitor is implements may not work with other company. Also, with global and hard competition it is always hard to define what security investments are important and are not affecting for the price of the product. Information security work should be planned well, overlays usually don’t work well enough.

6.4 Critical evaluation

Theoretical framework was conducted first in order to understand industrial internet and industrial internet cyber security. Information for industrial internet was easy to find and contribute, Saarelainen & Collin’s (2016) book *Teollinen Internet* (Industrial Internet) was published just before this thesis started. The book gave a good and easy to read framework also for the theoretical part of this research. Combining other articles and researches gave good view for industrial internet, its architecture and maturity. Information security framework for industrial internet was harder to conduct. There is not so many comprehensive industrial internet security researches. There are many shorter articles about IoT information security. Many of these articles are written in certain perspectives and decision was made if there is something for industrial internet security, e.g. privacy related security concerns were counted out almost fully because in industrial internet system, personal data is saved in principle only as a user information. Many of the IoT information security related articles offered only highlighted concerns or random lists about the security threats and mitigation. Difficulty was to find relevant information an prioritize it in order to answer industrial internet related information security concerns. IIRA framework (Industrial Internet Consortium, 2015) was also established in the year 2016 and for the first time that article gave a good reference architecture how to take security concerns into account in industrial internet architecture. This research helped to keep logic with security framework. Information security was also approached very general level, so many detailed things were left out. Research questions "*What is industrial internet by architecture and maturity?*" (SQ1) and *"What kind of cyber risks are associated with industrial internet?"* (SQ2) were answered well in theoretical framework. Challenge is also that within the framework of master thesis was that there was not time to analyse deeply all the potential research material. So, it can be a possibility that some relevant articles could have been missed.

Empirical study was done in order to know what is the status and believes about industrial internet and its information security in Finnish industrial vendor companies. Interviews was sensible to arrange with companies in order to answer main research questions. Of course, when big companies are interviewed, it is difficult to choose the right persons for the interview. In this research information technology, industrial automation, cyber security, industrial internet and general business leaders were interviewed, they have common that they are in the middle of the industrial internet change and responsible some way of its success. It was good to have different kind of representatives from different companies in order to create general model for industrial vendor segment. There might have had few more interviews, but with this scope strong similarities were found. In the semi-structured interviews, different kind of lists was formed to help respondents answer the questions. This was done, because it was known that not every respondent had a background from information security. Also, there is a risk that lists drives discussion in a certain direction, but created lists were extensive and it was said that answers can be also outside of the listed items. Half-structured interviews also were conducted for many few interviewees. Many of the respondents did not have concrete experience about finished industrial internet system and what it could bring as a finish product. This affects also that they do not have historical data about how the security should be done in the implementation phase. But also, a point of this research was to get information what are companies believes how cyber security should be taken into account when industrial internet technologies are implemented.

Some critical evaluation about the creation of theoretical framework and empirical part was already done above. It is good to evaluate that can the research results be generalized. This research was done mainly for the industrial vendor segment. But overall, when implementing industrial internet system, there are similar bottlenecks and risks regardless of the user segment. Of course, emphasis of the risk can be different. But overall results can be in very high level generalized for the use of industrial internet information security.

Biggest single grievance for the qualification for the results are that every industrial company is different. It means that whatever the model is, every company is creating their own kind of industrial internet system, using different technologies and outcome goals even might be different. That's why it is good to have different kind of lists about things to consider with the project, but the certain truth in company realization might be something different. It is good notice also that all the companies are at the same phase of industrial internet maturity (Figure 19). This research is not giving answers about, what if maturity is lower or higher. Information security risks might be different in different levels of industrial internet maturity. In this phase, smart connections have been created, so the main concern from information security perspective from the result point of view on smart devices and connections. But at the higher level of industrial internet maturity cloud and application level technology is implemented, different kind of information security risks rises also. So when evaluating these results, it has to be noticed that the mitigation methods are not exploitable in all companies that are implementing industrial internet technology.

6.5 Suggestions for further research

In order to make as versatile approach for industrial internet cyber security as possible, more research should be done. Here is some list about possible further research topics whose were poorly handled in this thesis:

- **Industrial internet information security shared responsibilities:** This research poorly answered and researched the topic about how responsibilities of the industrial internet security are or can be divided. This topic was really lightly gone through without a more detailed summary.

- **Information security recommendations at different levels of industrial internet maturity level:** In this research, all companies were at the same phase of industrial internet maturity. But how does the information security differ, when company is in the different phase of industrial internet maturity?

- **Detailed investment quantities for industrial internet information security work:** This topic was not gone through in this research. In addition to respondent feelings and opinions what is relevant of industrial internet security, they could have given emphasis about invested resources for top risks.

- **Best investment strategy for industrial internet security:** It is known that it is impossible to mitigate all the cyber risks of the industrial internet. But what is the most efficient way to invest in cyber security in comparison of mitigated risks.

REFERENCES

Abu-Elkheir, M., Hayajneh, M., Ali, N. (2013). Data Management for the Internet of Things: Design Primitives and Solution. 2013 Nov; 13(11): 15582–15612. doi: 10.3390/s131115582.

Ailisto, H. (2015). Teollisen Internetin ja Digitalisaation tilanne Suomessa. Tintti-seminaari 18.11.2015 luentomateriaali.

Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002) A Survey on Sensor Networks. IEEE Communications Magazine. August 2002. ISSN: 0163-6804. p. 102-114.

Attick, R. (2016). Intelligent Things >> It's all about machine learning. Blog post. Available: https://www.linkedin.com/pulse/intelligent-things-its-all-machine-learning-roger-attick?trk=hp-feed-article-title-like.

Babar, S., Mahalle, P., Stango, A., Prasad, N., Prasad, R. (2010). Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science, vol 89. pp 420-429.

Bonetto, R., Bui, N., Lakkundi, V., Olivereau, A., Serbanati, A., & Rossi, M. (2012). Secure Communication for Smart IoT Objects: Protocol Stacks , Use Cases and Practical Examples. IEEE WoWMoW2012.

Botta, A., Donato, W. De, Persico, V., & Pescap, A. (2014). On the Integration of Cloud Computing and Internet of Things. University of Napoli Federico II.

Bruner, J. (2013). *Industrial Internet*. Published by O´Reilly Media, Inc. March 2013 First Edition.

Buyya, R., Shin, C., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 1–18. http://doi.org/10.1016/j.future.2008.12.001

Cam-Winget, N., Sadeghi, A.-R., & Jin, Y. (2016). Invited - Can IoT Be Secured: Emerging Challenges in Connecting the Unconnected. *Proceedings of the 53rd Annual Design Automation Conference*, 122:1--122:6. http://doi.org/10.1145/2744769.2905004

Carty, M., Pimont, V., Schmid, D. (2012). Measuring the Value of Information Security Investments. IT@Intel White Paper (January 2012).

Chan, H., & Perrig, A. (2003). Security and Networks. Cernegie Mellon University, (October 2003).

Dimensional Research (2015). Internet of Things (IoT) Meets Big Data and Analytics : A Survey of IoT Stakeholders, (March 2015).

Chen, S., Member, S., Xu, H., Liu, D., Member, S., Hu, B., & Wang, H. (2014). A Vision of IoT: Applications , Challenges , and Opportunities With China Perspective, *1*(4), 349–359.

European Comission. (2015). EU:n tietosuojauudistuksen hyväksyminen vauhdittaa digitaalisten sisämarkkinoiden toteuttamista. IP/15/6321. Available: http://europa.eu/rapid/press-release_IP-15-6321_fi.htm.

Evans, D. (2011). The Internet of Things - How the Next Evolution of the Internet Is Changing Everything. Cisco white paper. Available: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Evans, P. C., & Annunziata, M. (2012). Industrial Internet: Pushing the Boundaries of Minds and Machines.

Fenn, J. (2011). Gartner's Hype Cycle Special Report for 2011. Published: 02 August 2011. ID: G00215667.

Gubbi, J., Buyya, R., & Marusic, S. (2012). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, (1), 1–19.

Hennink, M., Hutter, I., Bailey, A. (2010). Qualitative Research Methods. Published December 8th 2010 by Sage Publications. 304 pp.

Hermann, M., Pentek, T., Otto, B. 2015. Design Principles for Industrie 4.0 Scenarios: A Literature Review. Working Paper No. 01 / 2015. Technische Universität Dortmund. Available: http://www.snom.mb.tu-dortmund.de/cms/de/forschung/Arbeitsberichte/Design-Principles-for-Industrie-4_0-Scenarios.pdf.

Industrial Internet Consortium (2015). Industrial Internet Reference Architecture. Available: https://www.iiconsortium.org/IIRA.htm.

Jones, D. L., Wagstaff, K., Thompson, D., Addario, L. D., Navarro, R., Mattmann, C., Rebbapragada, U. (2012). Big Data Challenges for Large Radio Arrays.

Juhanko, J., Jurvansuu, Marko (toim.), Ahlqvist, Toni, Ailisto, Heikki, Alahuhta, Petteri, Collin, Jari, Halen, Marco, Heikkilä, Tapio, Kortelainen, Helena, Mäntylä, Martti, Seppälä, Timo, Sallinen, Mikko, Simons, Magnus ja Tuominen, Anu (5.1.2015). ”Suomalainen teollinen internet – haasteesta mahdollisuudeksi: taustoittava kooste”. ETLA Raportit No 42. http://pub.etla. /ETLA-Raportit-Reports-42.pdf

Kandukuri, B. R. (2009). Cloud Security Issues, 517–520. http://doi.org/10.1109/SCC.2009.84

Khan, R. Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In 2012 10th International Conference on Frontiers of Information Technology (FIT): Proceedings. (pp. 257-260). Institute of Electrical and Electronics Engineers Inc. DOI: 10.1109/FIT.2012.53

Kumar, J., & Patel, D. (2014). A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications*, *1*(2), 78–95. http://doi.org/10.5752/P.2316-9451.2013v1n2p78

Lee, J. (2014). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems A Cyber-Physical Systems architecture for Industry, (October 2016). http://doi.org/10.1016/j.mfglet.2014.12.001

Lehto, T. (2015). Konecranesin Lundmark: "Teollinen internet tulee nousemaan tai kaatumaan tietoturvaan". Talouselämä. Available: http://www.talouselama.fi/uutiset/konecranesin-lundmark-teollinen-internet-tulee-nousemaan-tai-kaatumaan-tietoturvaan-3473749.

Lu, C. (2014). Overview of Security and Privacy Issues in the Internet of Things. Available: http://www.cse.wustl.edu/~jain/cse574-14/ftp/security/index.html.

Lueth, K. (2014). IoT market segments – Biggest opportunities in industrial manufacturing. IOT Analytics. Available: https://iot-analytics.com/iot-market-segments-analysis/.

Lueth, K. (2015). The 10 most popular Internet of Things applications right now. IOT Analytics. Available: https://iot-analytics.com/10-internet-of-things-applications/.

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Thing. *Journal of Cyber Security and Mobility,* Vol. 1, 309–348.

Mamoon, Q., & Habaebi, M. H. (2015). Journal of Network and Computer Applications Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, *49*, 112–127. http://doi.org/10.1016/j.jnca.2014.11.011

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., Hung Byers, A. (2011). Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute report. May 2011. Available: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation.

Meola, A. (2016). The roles of cloud computing and fog computing in the Internet of Things revolution. Business Inside. Available: http://www.businessinsider.com/internet-of-things-cloud-computing-2016-10?r=US&IR=T&IR=T.

Miessler, D. (2014). HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Available: https://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.WRDGxFKB2fS.

Miorandi, D., Sicari, S., Pellegrini, F. De, & Chlamtac, I. (2012). Ad Hoc Networks Internet of things: Vision , applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. http://doi.org/10.1016/j.adhoc.2012.02.016

Mountreuil, B. (2012). Physical Internet Manifesto. Laval University, Quebec, Canada. Available: https://www.slideshare.net/physical_internet/physical-internet-manifesto-eng-version-1111-20121119-15252441.

OWASP (2013). OWASP Top 10 - 2013. Available: https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013.

OWASP (2017). About the Open Web Application Security Project. Available: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project.

Porter, M. E., & Heppelmann, J. E. (2015). How Smart, Connected Products Are Transforming Companies. *Harvard Business Review*, *93*(10), 96–114. Available: https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies.

Porter, M. E., & Heppelmann, J. E. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review.* Available: https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition.

Purdy, M., & Davarzani, L. (2015). The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity. Accenture.

PWC (2016). Adjusting the Lens on Economic Crime. Preparation brings opportunity back into focus. Global Economic Crime Survey 2016.

Rayman, N. (2014). The World's Top 5 Cybercrime Hotspots. Time Inc. Available: http://time.com/3087768/the-worlds-5-cybercrime-hotspots/.

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013). A systemic approach for IoT security. DOI: 10.1109/DCOSS.2013.78. Published in: Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*. http://doi.org/10.1016/j.comnet.2012.12.018

Rooheart, J. (2017). Cyber Crime to Reach $2 Trillion By 2019: What Can We Do? Business.com Technology. Available: https://www.business.com/articles/cyber-crime-to-reach-2-trillion-by-2019-what-can-we-do/.

Saarelainen, A., Collin, A. (2016) Teollinen Internet. ISBN:9789521428494. Alma Talent.

Saunders, M., Lewis, P. & Thornhill, A., 2009. Research Methods for Business Students, Pearson Education.

Seppälä, T., Collin, J., Martikainen, O. (2014). Teollinen Internet: Yritysten tietojärjestelmäarkkitehtuurien on aika uudistua. Digitaaliset ekosysteemit turbulenssissa -hanke, 19–24.

Shan, T. (2015). Internet of Things Maturity Model. Cloudonomic blog post. Available: http://cloudonomic.blogspot.fi/2015/02/internet-of-things-maturity-model.html.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. http://doi.org/10.1016/j.comnet.2014.11.008

Swan, M. (2012). Journal of Sensor Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0, 217–253. http://doi.org/10.3390/jsan1030217

Sweeney, L. (2002). *k*-Anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570

Telekom (2016). White paper: Security for industrial Internet of Things. Available: https://www.telekom.com/en/company/internet-of-things.

The Telegraph. (2010). Computer worm infects Iran's nuclear station. The Telegraph. Available: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8026284/Computer-worm-infects-Irans-nuclear-station.html.

Tiilikainen, S., Manner, J., (2013). Suomen automaatioverkkojen haavoittuvuus - Raportti Internetissä julkisesti esillä olevista automaatiolaitteista. Aalot Univeristy. Available: https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf.

Viitamo, E. (2014). Service productivity, technology and organization: Converting theory to praxis. ETLA Working Papers No 26. http://pub.etla. /ETLA-Working-Papers-26.pdf

Weber, J. (2016). Fundamentals of IoT device management. IoT Design. Available: http://iotdesign.embedded-computing.com/articles/fundamentals-of-iot-device-management/.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. http://doi.org/10.1016/j.clsr.2009.11.008

World Economics Forum (2015). Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, (January 2015).

World Energy Council (2016). The road to resilance: Managing cyber risks. World Energy Perspectives. Published: September 2016. Available: https://www.worldenergy.org/publications/2016/the-road-to-resilience-managing-cyber-risks/.

Yousuf, T., Mahmoud, R., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures, *5*(4), 608–616. International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2015). Sensing as a Service and Big Data.

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired.com. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

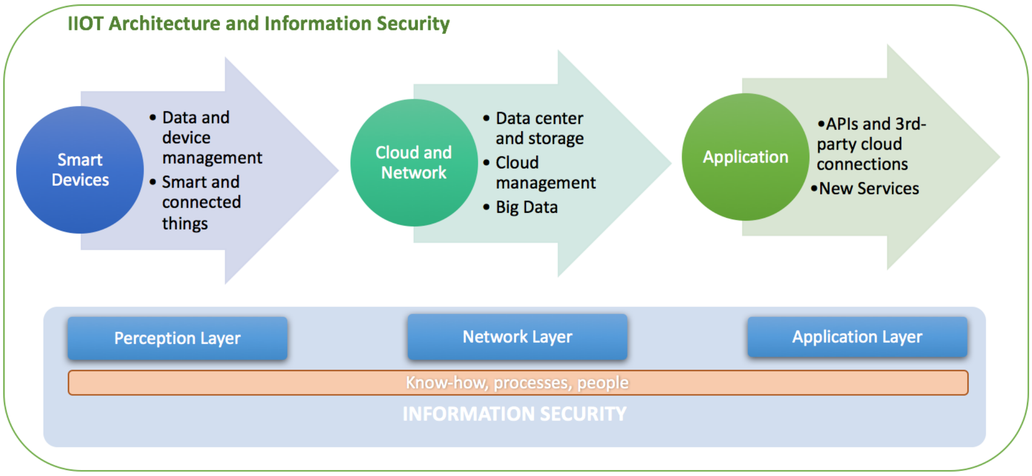
Zhao, K., & Ge, L. (2013). A survey on the internet of things security. *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 663–667. http://doi.org/10.1109/CIS.2013.145

ZigBee (2017). What is ZigBee? ZigBee alliance. Available: http://www.zigbee.org/what-is-zigbee/.

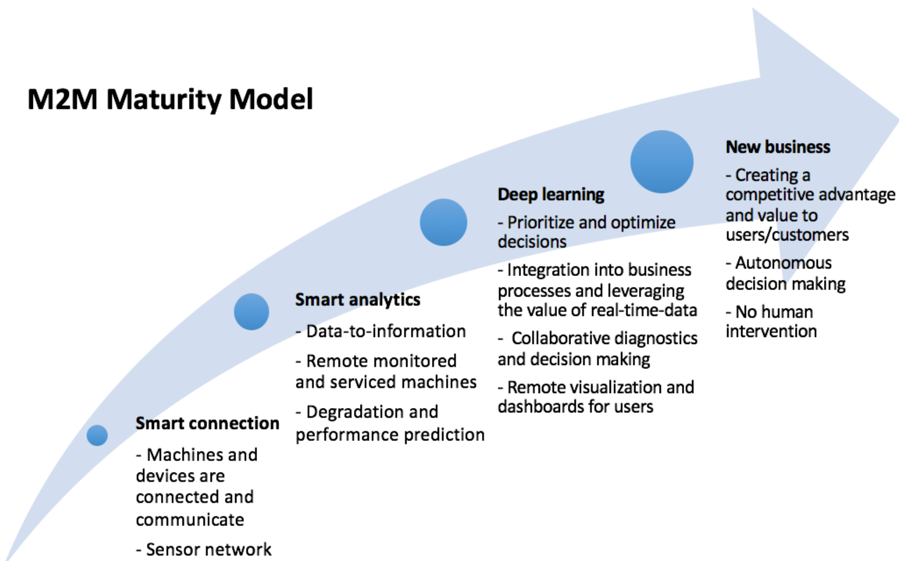
APPENDIX A: SEMI STRUCTURED INTERVIEW

1. Kuka olet ja millainen tausta sinulla on? Mitä vastuualueita sinulla on?

2. Miten teollinen internet ilmenee yrityksessä ja miten näet teollisen internetin kypsyyden tason?
   - Jatkokysymykset: Koska usein arkkitehtuurin eri vaiheissa ollaan eri tasoilla niin miten yrityksen osaaminen ja prosessit ovat kehittyneet eri vaiheissa? Esimerkiksi missä kypsyystasolla ollaan edellä ja missä jäljessä?



Teollisen internetin arkkitehtuuri ja tietoturvallisuustasot.



Teollisen internetin maturiteetti.

3. Miksi teollisen internetin tietoturvaan tulisi investoida?
    - Jatkokysymys: Nähdäänkö sellaisia merkittäviä riskejä, jotka ovat nimenomaan merkittäviä teollisen internetin käyttöönotossa verrattuna nykyisiin tai muihin toimintatapoihin?

4. Onko niin isoja tai suuria riskejä, ettei uskalleta ottaa teollista intranetiä käyttöön niin laajasti kuin olisi järkevää?

5. Onko teollisen internetin tietoturvaan lähestytty jonkin tietyn mallin mukaan? Minkälaisen?

6. Mitkä liiketoimintariskit nousevat vaikuttavimpina esiin teollisen internetin näkökulmasta? (Taulukko1)
    - Jatkokysymys: Miksi nämä tietoturvariskit koetaan merkittävinä?
    - Nähdäänkö tietoturvariskit vakavina, eli mikä ajatus niiden merkittävyydestä ja todennäköisyydestä?

7. Mitkä edellä mainituista riskeistä tai muista osuvat eri osa-alueisiin teollisen internetin arkkitehtuurissa (sijoitetaan riskit esimerkiksi komponentti-, verkko- tai sovellustasolle, tai näiden väliin)? (Taulukko1)

8. Mitkä tietoturvariskit nousevat vaikuttavimpina esiin teollisen internetin näkökulmasta? (top3) (Taulukko 2)
    - Jatkokysymys: Miksi nämä tietoturvariskit koetaan merkittävinä?

9. Mitkä edellä mainituista riskeistä tai muista osuvat eri osa-alueisiin teollisen internetin arkkitehtuurissa (sijoitetaan riskit esimerkiksi komponentti-, verkko- tai sovellustasolle, tai näiden väliin)? (Taulukko2)

10. Missä teollisen internetin arkkitehtuurin osa-alueella yrityksenne (Industrial vendor –toimija) tietoturvaan panostaminen on erityisen tärkeää?
    - Jatkokysymys; onko tietyillä alueilla Industrial Vendor näkökulmasta tietoturvaan panostaminen tärkeää ja jossakin vaiheessa enemmän esimerkiksi enemmän teknologiapartnereiden (esim. Pilvipalvelutoimittaja) vastuulla?

11. Mitkä ovat merkittävimpien (top3) riskien hallintakeinot? Ensimmäisen tason; komponenttitaso; siirtotaso;. Miksi nähdään tämän tyyppiset hallintakeinot tärkeinä?

Taulukko1. Liiketoimintariskit

Tietoturvariskien seurauksen liiketoiminnan näkökulmasta

Business

- Reputation
- Compliance risk (Losing opportunities/customers because of the cannot fulfil standards)
- Information risk:
    1. Theft of customer data
    2. Privacy
    3. Damaged intellectual property
    4. Integrity (data of machines and applications)
- Availability and interruption of production (also in customer environment)

Taulukko2. Tietoturvariskit

***Riskien listaaminen** (Babar et. al. 2010, Sicari et al. 2014):*

- *Haavoittuvuudet pilvirajapinnassa*
- *Identiteetinhallinta (autentikointi, valtuuttaminen, kulunvalvonta, pääsynhallinta)*
- *Kryptatyn liikenteen puutteet*
- *Turvallinen tallentaminen (luotettavuus, avaintenhallinta, yhdenmukaisuus, saatavuus)*
- *Tietoliikenteen uhat, tietoverkon haavoittuvuudet*
- *Myöhäinen sidonta (late binding) (nimeämismekanismit, nimien ja järjestelmin yhteensovittaminen, implisiittisten nimien hallinta)*
- *Fyysinen uhka (microproping, käänteinen suunnittelu)*
- *Sulautettu turvallisuus (side channeling, datan peukalointi, komponenttien autentikointi, turvallinen ympäristö)*
- *Mobiiliturvallisuu, mobiilikäyttöliittymien haavoittuvuudet*
- *Yksityisyys ja tietosuojan puutteet*
- *Heikot suojausasetukset*